Nortel Secure Network Access Switch

Using the Command Line Interface

Release: 2.0
Document Revision: 03.01

www.nortel.com

NN47230-100 320818-D

Nortel Secure Network Access Switch
Release: 2.0
Publication: NN47230-100
Document status: Standard
Document release date: 28 July 2008

Sourced in Canada, the United States of America, and India

Contents

Software license

This section contains the Nortel Networks software license.

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who

uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

New in this release

The following sections detail what's new in *Nortel Secure Network Access Using the Command Line Interface*, (NN47230-100) for Release 2.0.

Features

This is the second standard release of the document. See the following sections for information, which are added in this Release.

On-the-fly SRS Policy Change—When a security policy is modified on the SNAS using the administrative tool the policy is updated on the Nortel Health Agent running on the logged in operating systems. For more information, See the "Configuring the Nortel Health Agent check" (page 92).

Multi-OS Applet Support—The Nortel Health captive portal applet supports Windows and non-Windows operating systems. For non-Windows operating systems the applet supports collecting operating systems information and VLAN transition. for more information, see the “Multi-OS Applet Support” (page 32).

Other changes

No changes.

Introduction

Nortel* Secure Network Access (Nortel SNAS) is a clientless solution that provides seamless, secure access to the corporate network from inside or outside that network. The Nortel SNAS combines multiple hardware devices and software components to support the following features:

- partitions the network resources into access zones (authentication, remediation, and full access)
- provides continual device integrity checking using Nortel Health Agent
- supports both dynamic and static IP clients

The Nortel Secure Network Access Switch 4050or 4070 (Nortel SNAS 4050 or 4070) controls operation of the Nortel SNAS.

This user guide covers the process of implementing the Nortel SNAS using the Nortel SNAS 4050 or 4070 for Nortel Secure Network Access Switch Software Release 2.0. The document includes the following information:

- overview of the role of the Nortel SNAS 4050 or 4070 in the Nortel SNAS
- initial setup
- configuring authentication, authorization, and accounting (AAA) features
- managing system users
- customizing the portal
- upgrading the software
- logging and monitoring
- troubleshooting installation and operation

The document provides instructions for initializing and customizing the features using the Command Line Interface (CLI). To learn the basic structure and operation of the Nortel SNAS CLI, refer to “CLI reference” (page 413). This reference guide provides links to where the function

and syntax of each CLI command are described in the document. For information on accessing the CLI, see "The Command Line Interface" (page 377).

BBI is a graphical user interface (GUI) that runs in an online, interactive mode. BBI allows the management of multiple devices (for example, the Nortel SNAS) from one application. For information about using BBI to configure and manage Nortel SNAS, see *Nortel Secure Network Access Switch Configuration — Using the BBI*, (NN47230-500).

Before you begin

This guide is intended for network administrators who have the following background:

- basic knowledge of networks, Ethernet bridging, and IP routing
- familiarity with networking concepts and terminology
- experience with windowing systems or GUIs
- basic knowledge of network topologies

Before using this guide, you must complete the following procedures. For a new switch:

Step	Action
1	Install the switch. For installation instructions, see *Nortel Secure Network Access Switch 4050 Installation Guide* , (NN47230-300).
2	Connect the switch to the network. For more information, see "The Command Line Interface" (page 377).
	--End--

Ensure that you are running the latest version of Nortel SNAS software. For information about upgrading the Nortel SNAS, see "Upgrading or reinstalling the software" (page 367).

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Enter text based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping <ip_address>`**, you enter **`ping 192.32.10.12`**
bold text	Objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, tabs, and menu items.
`bold Courier text`	Command names, options, and text that you must enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip {alerts|routes}`**.
braces ({})	Required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`show ip {alerts|routes}`**, you must enter either **`show ip alerts`** or **`show ip routes`**, but not both.
brackets ([ ])	Optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ip interfaces [-alerts]`**, you can enter either **`show ip interfaces`** or **`show ip interfaces -alerts`**.
ellipsis points (. . .)	Repeat the last element of the command as needed. Example: If the command syntax is **`ethernet/2/1 [ <parameter> <value> ]...`**, you enter **`ethernet/2/1`** and as many parameter-value pairs as needed.

italic text	Variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`show at <valid_route>`**, **`valid_route`** is one variable and you substitute one value for it.
`plain Courier text`	Command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Menu paths. Example: **Protocols > IP** identifies the **IP** command on the **Protocols** menu.
vertical line (|)	Options for command keywords and arguments. Enter only one of the options. Do not type the vertical line when entering the command. Example: If the command syntax is **`show ip {alerts|routes}`**, you enter either **`show ip alerts`** or **`show ip routes`**, but not both.

Related information

This section lists information sources that relate to this document.

Publications

Refer to the following publications for information on the Nortel SNAS:

- *Nortel Secure Network Access Solution Guide*, (NN47230-200)
- *Nortel Secure Network Access Switch 4050 Installation Guide* , (NN47230-300).
- *Nortel Secure Network Access Switch 4050 User Guide for the CLI (NN47230-100)*,
- *Installing and Using the Security*,
- *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.1*,
- *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8* ,

- *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.6.1 (NN47230-400)*,
- *Release Notes for Enterprise Switch Manager (ESM), Software Release 5.2 (209960-H)*,
- *Using Enterprise Switch Manager Release 5.1 (208963-F)*,
- *Nortel Secure Network Access Switch Configuration — Using the BBI*, (NN47230-500).

Online

To access Nortel technical documentation online, go to the Nortel web site:

http://www.nortel.com/support

You can download current versions of technical documentation. To locate documents, browse by category or search using the product name or number.

You can print the technical manuals and release notes free, directly from the Internet. Use Adobe* Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems site at http://www.adobe.com to download a free copy of Adobe Reader.

How to get help

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel service program, use the http://www.nortel.com/help web page to locate information to contact Nortel for assistance:

- To obtain Nortel Technical Support contact information, click the **CONTACT US** link on the left side of the page.
- To call a Nortel Technical Solutions Center for assistance, click the **CALL US** link on the left side of the page to find the telephone number for your region.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate the ERC for your product or service, go to the http://www.nortel.com/helpweb page and follow these links:

Step	Action
1	Click **CONTACT US** on the left side of the **HELP** web page.
2	Click **Technical Support** on the **CONTACT US** web page.
3	Click **Express Routing Codes** on the **TECHNICAL SUPPORT** web page.

--End--

Overview

The Nortel Secure Network Access Solution Release 2.0 features are mapped to the relevant section(s) in this guide in the following table. For information on the Nortel SNAS Release 1.6.1 see *Release Notes for Nortel Secure Network Access Solution Release 1.6.1, NN47230-400*, (formerly 320850).

Table 1
Features on NSNA

Feature	Section
Performance and scalability enhancements: 20,000 concurrent users	Not applicable.
Support for hubs	"Configuring local DHCP services" (page 115), "Hub DHCP subnet type" (page 118)
Support for Nortel Ethernet Switch models - 325 / 425 / 450 / 470 and 2500 series and Ethernet Routing Switch models - 4500 series, 5500 series, 8300 and 8600.	"Configuring local DHCP services" (page 115), "Hub DHCP subnet type" (page 118)
Support for WLAN Controller	"Configuring local DHCP services" (page 115), "Hub DHCP subnet type" (page 118)
Support of RADIUS server	"Configuration of the RADIUS server" (page 127)
Support of Microsoft NAP Interoperability	"Configuration of Microsoft NAP Interoperability" (page 139)
Nortel Health Agent Run-Once, Continuous and Never modes	"Configuring groups" (page 156), "Managing the local MAC database" (page 206)
Support for MAC OSX, Linux OS, and non-interactive devices	"Configuring groups" (page 156)
MAC address policy services	"Configuring groups" (page 156), "Managing the local MAC database" (page 206)
Flexible deployment: Filter only and VLAN and filters deployment	"Nortel SNAS enforcement types" (page 28), "Configuring groups" (page 156)

ATTENTION
Switches that support the Switch to Nortel SNAS Communication Protocol (SSCP) are referred to as NSNA network access devices in this document. Generally, NSNA network access devices are the Ethernet Routing Switch 5500 Series and the Ethernet Routing Switch 8300. Specifically, Release 1.6.1 features are supported by the Ethernet Routing Switch 5500 Series, Release 5.0.2 and later.

ATTENTION
The character combination "**<**" appears instead of the character "**<**" in several command strings in this document. For example, **<DN>** rather than **<DN>**. Resolution is under investigation.

This chapter includes the following topics:

The Nortel SNAS

Nortel Secure Network Access Solution (Nortel SNAS) is a protective framework to completely secure the network from endpoint vulnerability. The Nortel SNAS addresses endpoint security and enforces policy compliance. Nortel SNAS delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, user identity, and session context. Nortel SNAS enforces policy compliance, such as for Sarbanes-Oxley and COBIT, ensuring that the required anti-virus applications or software patches are installed before users are granted network access.

For Nortel, success is delivering technologies providing secure access to your information using security-compliant systems. Your success is measured by increased employee productivity and lower network operations costs. Nortel's solutions provide your organization with the network intelligence required for success.

Elements of the Nortel SNAS

The following devices are essential elements of the Nortel SNAS:

- Nortel Secure Network Access Switch 4050or 4070 (Nortel SNAS 4050 or 4070), which acts as the Policy Decision Point
- network access devices, which acts as the Policy Enforcement Point
  - Ethernet Routing Switch 8300
  - Ethernet Routing Switch 4500, 5510, 5520, or 5530

  ATTENTION
  NSNA Release 1.6.1 does not currently support the Ethernet Routing Switch 8300 as a Policy Enforcement Point.
- RADIUS, DHCP, and DNS servers

The following devices are additional, optional elements of the Nortel SNAS:

- remediation server
- corporate authentication services such as LDAP or RADIUS services

Each Nortel SNAS device can support up to five network access devices.

Supported users

The Nortel SNAS supports the following types of users:

- PCs using the following operating systems:
  - Windows 2000 SP4
  - Windows XP SP2
  - Linux
  - MAC OS
  - Vista

  The Nortel SNAS supports the following browsers:
  - Internet Explorer version 6.0 or later
  - Netscape Navigator version 7.3 or later
  - Mozilla Firefox version 1.0.6 or later

  Java Runtime Environment (JRE) for all browsers:
  - JRE 1.6.0_04 or later
- VoIP phones

— Nortel IP Phone 2002

— Nortel IP Phone 2004

— Nortel IP Phone 2007

See *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.6.1 (NN47230-400)*, for the minimum firmware versions required for the IP Phones operating with different call servers.

Each Nortel SNAS -enabled port on a network access devices can support one PC (untagged traffic) and one IP Phone (tagged traffic). Softphone traffic is considered to be the same as PC traffic (untagged).

ATTENTION
Where there is both an IP Phone and a PC, the PC must be connected through the 3-port switch on the IP Phone.

Supporting additional users with the software license file

The standard Nortel SNAS 4050 implementation can support up to 200 authenticated user sessions. To support additional users on your Nortel SNAS 4050 switch, you must obtain a Nortel SNA software license file. The software license file contains a software license key that you must enter into the Nortel SNAS 4050 switch to activate support for the additional users. The file can support an additional 100, 250, 500, or 1000 users.

ATTENTION
An authenticated IP Phone is considered to be a licensed user.

Your unique software license key is based on your switch MAC address. Before you obtain your software license file, first record the MAC address for the Nortel Secure Network Access Switch to be upgraded. To find the MAC address in the Command Line Interface, use the **`/info/local`** command.

To obtain your software license file, contact Nortel to order the Nortel SNA Software License Certificate. Follow the instructions on this certificate to obtain your software license file.

After you obtain the software license file from Nortel, you must copy the entire license key to the switch using the CLI or the BBI. When you copy the license key, ensure you include the `BEGIN LICENSE` and `END LICENSE` lines.

To copy the license key using the CLI, use the following command:

`/cfg/sys/host <host ID> license <key>`

The following shows a sample display of the CLI interface when copying the license key:

```
>> Main# cfg/sys/host
Enter Host number:  1
>> iSD host 1# license

Paste the license, press Enter to create a new line,
and then type "..." (without the quotation marks)
to terminate.
> -----BEGIN LICENSE-----
> U4GsdGVkX36AJpnd8KL4iImtRzBvZy+iANDzxog22+vq6Qx4aawSl4FVQo
> lXYlsNNFJpYW/vl3osvNPXhzcLV2E9hNHlqirkzc5aLDJ+2xYpK/BRDrMZ
> 86OQvdBMyer53xgq8Kk/5BvoFcQYvEC/yWrFyrmZr4XPtAr3qmuZ8UxLqJ
> 0x7PUrp6tVI=
> -----END LICENSE-----
> ...
License loaded
```

For more information, see “Configuring the Nortel SNAS host” (page 264).

To copy the license key using the BBI, use the Install New License screen (**System > Hosts > *host* > Install New License**).

To view the license using BBI, in the cluster select **Cluster > Hosts > License** from the menu. For more information, see *Nortel Secure Network Access Switch Configuration — Using the BBI*, (NN47230-500).

Role of the Nortel SNAS

The Nortel SNAS helps protect the network by ensuring endpoint compliance for devices that connect to the network.

Before allowing a device to have full network access, the Nortel SNAS checks user credentials and host integrity against predefined corporate policy criteria. Through tight integration with network access devices, the Nortel SNAS can:

- dynamically move the user into a quarantine VLAN
- dynamically grant the user full or limited network access
- dynamically apply per port firewall rules that apply to a device’s connection

Once a device has been granted network access, the Nortel SNAS continually monitors the health status of the device to ensure continued compliance. If a device falls out of compliance, the Nortel SNAS can dynamically move the device into a quarantine or remediation VLAN.

Nortel SNAS functions

The Nortel SNAS performs the following functions:

- Acts as a web server portal, which is accessed by users in clientless mode for authentication and host integrity check and which sends remediation instructions and guidelines to endpoint clients if they fail the host integrity check.
- Communicates with backend authentication servers to identify authorized users and levels of access.
- Acts as a policy server, which communicates with the Nortel Health Agent applet that verifies host integrity.
- Instructs the network access devices to move clients to the appropriate enforcement zones.
- Can be a DNS proxy in the Red VLAN when the Nortel SNAS functions as a captive portal
- Supports the RADIUS server
- Supports Microsoft NAP Interoperability.
- Performs session management.
- Monitors the health of clients and switches.
- Performs logging and auditing functions.
- Provides High Availability (HA) through IPmig protocol.

Nortel SNAS enforcement types

Nortel SNAS provides several enforcement types for restricting access to the network.

- **VLANs and filters** uses a combination of VLANs and filters to provide enforcement. It is available with NSNA network access devices; that is, devices that support SSCP (Switch-SNAS Communication Protocol), SSCP-Lite, and 802.1x switches.
- **Filters only** uses only filters to provide enforcement. It is available with NSNA network access devices.
- NSNA network access devices including Nortel Ethernet Switch models - 325, 425, 450, 470 and 2500 series and Ethernet Routing Switch models - 4500 series, 5500 series, 8300 and 8600 as well as third-party switches.

VLANs and filters

Four type of Layer 2 or Layer 3 VLANs are configured for **VLANs and filters** enforcement:

- Red—extremely restricted access. If the default filters are used, the user can communicate only with the Nortel SNAS and the Windows domain controller network. There is one Red VLAN for each network access devices.
- Yellow—restricted access for remediation purposes if the client PC fails the host integrity check. Depending on the filters and Nortel Health Agent rules configured for the network, the client may be directed to a remediation server participating in the Yellow VLAN. There can be up to five Yellow VLANs for each network access devices. Each user group is associated with only one Yellow VLAN.
- Green—full access, in accordance with the user's access privileges. There can be up to five Green VLANs for each network access devices.
- VoIP—automatic access for VoIP traffic. The network access devices places VoIP calls in a VoIP VLAN without submitting them to the Nortel SNAS authentication and authorization process.

When a client attempts to connect to the network, the network access devices places the client in its Red VLAN. The Nortel SNAS authenticates the client. By default, the Nortel SNAS then downloads a Nortel Health Agent applet to check the integrity of the client host. If the integrity check fails, the Nortel SNAS instructs the network access devices to move the client to a Yellow VLAN, with its associated filter. If the integrity check succeeds, the Nortel SNAS instructs the network access devices to move the client to a Green VLAN, with its associated filter. The network access devices applies the filters when it changes the port membership.

The VoIP filters allow IP phone traffic into preconfigured VoIP VLANs, for VoIP communication only.

The default filters can be modified to accommodate network requirements, such as Quality of Service (QoS) or specific workstation boot processes and network communications.

For information about configuring VLANs and filters on the network access devices, see *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.1*, or *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8* , .

To configure the Nortel SNAS for **VLANs and filters** enforcement, see "Configuring groups" (page 156), **enftype**.

Filters only

Filters only enforcement uses two VLANs: Red and VoIP. A client computer is placed in the Red VLAN where it is held pending successful authentication. If successful, Nortel Health Agent integrity checking can be used to determine if remediation is required. Filters are applied to direct the client to the appropriate network resources but the client remains in the same VLAN regardless of its status. This contrasts with **VLANs and filters** where the client is moved to another VLAN in addition to applying filters. **Filters only** handles IP phones in the same manner as **VLANs and filters**.

With **Filters only**, there is less network configuration than with **VLANs and filters** because there are only two VLANs (Red and VoIP) to configure. However, the double layer of protection afforded with **VLANs and filters** is not provided.

To configure the Nortel SNAS for **Filters only** enforcement, see "Configuring groups" (page 156), **enftype**. Though configuring for **Filters only** can result in higher DNS demands on the Nortel SNAS, using the filter DHCP subnet type maintains these demands at the same level as with **VLANs and filters**: for more information, see "Configuring local DHCP services" (page 115).

DHCP hub subnet

DHCP hub subnet enforcement allows the Nortel SNAS to operate with a broader range of Nortel ethernet switches as well as third party network access devices. Unlike **VLANs and filters** and **Filters only** enforcement, **DHCP hub subnet** enforcement does not require SSCP support on the network access device.

The **DHCP hub subnet** configuration is an integral component of the DHCP services provided by the Nortel SNAS. For more information, see "Configuring local DHCP services" (page 115).

Groups and profiles

Users are organized in groups. In the user gorup we can specify Locaion also. Group membership determines:

- user access rights
  Within the group, extended profiles further refine access rights depending on the outcome of the Nortel Health Agent checks.
- number of sessions allowed
- the Nortel Health Agent SRS rule to be applied
- what on the portal page after the user has been authenticated

For information about configuring groups and extended profiles on the Nortel SNAS, see “Configuring groups and profiles” (page 149).

Authentication methods

You can configure more than one authentication method within a Nortel SNAS domain. Nortel Secure Network Access Switch Software Release 2.0 supports the following authentication methods:

- external database
  - Remote Authentication Dial-In User Service (RADIUS)
  - Lightweight Directory Access Protocol (LDAP)

  The Nortel SNAS authenticates the user by sending a query to an external RADIUS or LDAP server. This makes it possible to use authentication databases already existing within the intranet. The Nortel SNAS device includes username and password in the query and requires the name of one or more access groups in return. The name of the RADIUS and LDAP access group attribute is configurable.
- local authentication databases
  - Portal authentication: The Nortel SNAS can store up to 1,000 user authentication entries in its own portal database. Each entry in the database specifies a username, password, and relevant access group.
    Use the local authentication method if no external authentication databases exist, for testing purposes, for speedy deployment, or as a fallback for external database queries. You can also use the local database for authorization only, if an external server provides authentication services but cannot be configured to return a list of authorized groups.
  - MAC authentication: The media access control (MAC) address of the end point device can be used for authentication. The Nortel SNAS 4050 can store over 10,000 MAC addresses and support over 2,000 concurrent MAC sessions. Each entry in the database specifies a MAC address, IP type, device type, and group name(s). You can optionally specify a user name, IP address of the device, comments, and the IP address, unit, and port of the switch to which the device is attached.

  You can populate the local authentication databases by manually adding entries on the Nortel SNAS, or you can import a database from a TFTP/FTP/SCP/SFTP server.

For information about configuring authentication on the Nortel SNAS, see “Configuring authentication” (page 171).

For more information about the way Nortel SNAS controls network access, see *Nortel Secure Network Access Solution Guide*, (NN47230-200).

Nortel Health Agent host integrity check

The Nortel Health Agent application checks client host integrity by verifying that the components you have specified are required for the client's personal firewall (executables, DLLs, configuration files, and so on) are installed and active on the client PC. You specify the required component entities and engineering rules by configuring a Software Requirement Set (SRS) rule and mapping the rule to a user group.

After a client gets authenticated, the Nortel SNAS downloads a Nortel Health Agent as an applet to the client PC. The Nortel Health Agent applet fetches the SRS rule applicable for the group to which the authenticated user belongs, so that Nortel Health Agent can perform the appropriate host integrity check. The Nortel Health Agent applet reports the result of the host integrity check to the Nortel SNAS.

If the required components are present on the client machine, Nortel Health Agent reports that the SRS rule check succeeded. The Nortel SNAS then instructs the network access devices to permit access to intranet resources in accordance with the user group's access privileges. The Nortel SNAS also requests the Nortel Health Agent applet to redo a DHCP request in order to renew the client's DHCP lease with the network access devices.

If the required components are not present on the client machine, Nortel Health Agent reports that the SRS rule check failed. You configure behavior following host integrity check failure: The session can be torn down, or the Nortel SNAS can instruct the network access devices to grant the client restricted access to the network for remediation purposes.

The Nortel Health Agent applet repeats the host integrity check periodically throughout the client session. If the check fails at any time, the client is either evicted or quarantined, depending on the behavior you have configured. The recheck interval is configurable.

For information about configuring the Nortel Health Agent host integrity check, see "Configuring the Nortel Health Agent check" (page 92). For information about configuring the SRS rules, see information about the Nortel Health Agent SRS Builder in *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, . For information about mapping an SRS rule to a group, see "Configuring groups" (page 156).

Multi-OS Applet Support

The Nortel Health captive portal applet supports Windows and non-Windows operating systems. For non-Windows operating systems the applet supports collecting operating systems information and VLAN transition.

The “Multi-OS Support" feature allows the Nortel Health Agent to identify Linux operating system or Macintosh operating system users and collect the necessary information. The Nortel Health Agent is allowed to identify the operating system as Linux or Macintosh and collect the device specific information and also performs additional compliance checks for those operating systems.

The following types of Linux operating system are supported:

- RedHat Enterprise Linux 4
- RedHat Enterprise Linux 3
- Fedora Core 6
- Fedora Core 5
- SUSE Linux Enterprise 10

The following types of Macintosh operating system are supported:

- Mac OS X Server v10.5 Leopard
- Mac OS X Server v10.4 Tiger
- Mac OS X v10.3 Panther
- Mac OS X v10.2
- Mac OS 9

Communication channels

Communications between the Nortel SNAS and key elements of the Nortel SNAS are secure and encrypted. Table 2 "Communication channels in the Nortel SNAS network" (page 33) shows the communication channels in the network.

Table 2
Communication channels in the Nortel SNAS network

Communication	Communication protocol
Between Nortel SNAS and edge switches	SSH
Between Nortel SNAS devices in a cluster	TCP and UDP
Between Nortel SNAS and client PC (Nortel Health Agent applet)	SSL/TLS
For Nortel SNAS	BBI
From edge switch to EPM	SNMPv3 Inform

Table 2
Communication channels in the Nortel SNAS network (cont'd.)

Communication	Communication protocol
From EPM to edge switch	Telnet over SSH
From authorized endpoint to DHCP server	UDP

Telnet or SSH can be used for management communications between remote PCs and the Nortel SNAS devices.

About SSH The Secure Shell (SSH) protocol provides secure and encrypted communication between the Nortel SNAS and the network access devices, and between Nortel SNAS devices and remote management PCs not using Telnet.

SSH uses either password authentication or public key authentication. With public key authentication, pairs of public/private SSH host keys protect against "man in the middle" attacks by providing a mechanism for the SSH client to authenticate the server. SSH clients keep track of the public keys to be used to authenticate different SSH server hosts.

SSH clients in the Nortel SNAS network do not silently accept new keys from previously unknown server hosts. Instead, they refuse the connection if the key does not match their known hosts.

The Nortel SNAS supports the use of three different SSH host key types:

- RSA1
- RSA
- DSA
  SSH protocol version 1 always uses RSA1 keys. SSH protocol version 2 uses either RSA or DSA keys.

For management communications in the Nortel SNAS, the Nortel SNAS can act both as SSH server (when a user connects to the CLI using an SSH client) and as SSH client (when the Nortel SNAS initiates file or data transfers using the SCP or SFTP protocols).

For information about managing SSH keys for communication between the Nortel SNAS and the network access devices, see "Managing SSH keys" (page 68).

For information about managing SSH keys for Nortel SNAS management communications, see "Configuring Nortel SNAS host SSH keys" (page 284).

Nortel SNAS clusters

For Release 1.6.1

A cluster is a group of Nortel SNAS 4050 devices that share the same configuration parameters. Nortel Secure Network Access Switch Software Release 1.6.1 supports four Nortel SNAS 4050 devices, or nodes, in a cluster. A network can contain multiple clusters.

For Release 2.0

A cluster is a group of Nortel SNAS 4050 or 4070 devices that share the same configuration parameters. Nortel Secure Network Access Switch Software Release 2.0 supports a combination of four Nortel SNAS 4050 and 4070 devices, or nodes, in a cluster. A Nortel SNAS network can contain multiple clusters.

Clustering offers the following benefits:

- manageability—The cluster is a single, seamless unit that automatically pushes configuration changes to its members.
- scalability—The Nortel SNAS nodes in a cluster share the burden of resource-intensive operations. The cluster distributes control of the network access devices between the Nortel SNAS nodes and distributes handling of session logon. As a result, Nortel SNAS devices in a cluster can control more switches and handle more user sessions.
- fault tolerance—If a Nortel SNAS device fails, the failure is detected by the other node in the cluster, which takes over the switch control and session handling functions of the failed device. As long as there is one running Nortel SNAS, no sessions will be lost.

The devices in the cluster can be located anywhere in the network and do not have to be physically connected to each other. All the Nortel SNAS devices in the cluster must be in the same subnet. The cluster is created during initial setup of the second node, when you specify that the setup is a join operation and you associate the node with an existing Management IP address (MIP).

For more information about Nortel SNAS IP addresses, see “About the IP addresses” (page 42). For information about adding a node to a cluster, see “Adding a Nortel SNAS device to a cluster” (page 50).

Interface configuration

The Nortel SNAS must interface to two kinds of traffic: client and management. The interface to the client side handles traffic between the Nortel Health Agent applet on the client and the portal. The interface to

the management side handles Nortel SNAS management traffic (traffic connecting the Nortel SNAS to internal resources and configuring the Nortel SNAS from a management station).

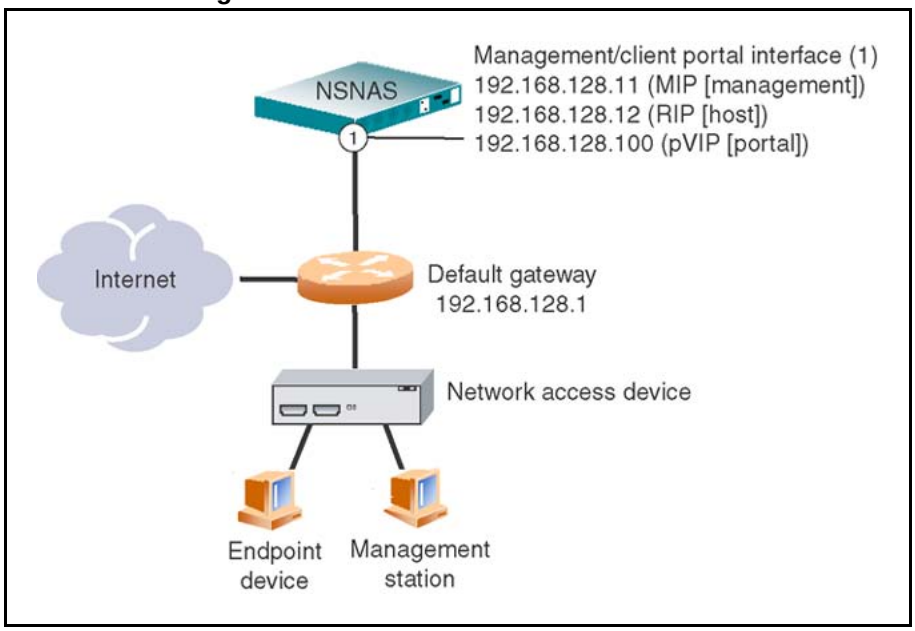
The Nortel SNAS supports what is known as an ***One armed*** configuration. The following section describes this configuration type.

One armed configuration

In an one armed configuration, the Nortel SNAS has only one interface, which acts as both the client portal interface and the management traffic interface.

Figure 1 "One armed configuration" (page 36) illustrates a one-armed configuration.

Figure 1
One armed configuration



Nortel SNAS configuration and management tools

You can use a number of device and network management tools to configure and manage the Nortel SNAS:

- Command Line Interface (CLI)
  You must use the CLI to perform initial setup on the Nortel SNAS and to set up the Secure Shell (SSH) connection between the Nortel SNAS and the network access devices, and between the Nortel SNAS and the GUI management tool. You can then continue to use the CLI to configure and manage the Nortel SNAS, or you can use the GUI.

The configuration chapters in this User Guide describe the specific CLI commands used to configure the Nortel SNAS. For general information about using the CLI, see "The Command Line Interface" (page 377).

- Security & Routing Element Manager (SREM)
  The SREM is a GUI application you can use to configure and manage the Nortel SNAS.
  For information about configuring the Nortel SNAS using the SREM, see *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, . For general information about installing and using the SREM, see *Installing and Using the Security*, .
- Browser Based Interface (BBI)
  The BBI is a web browser application you can use to configure and manage the Nortel SNAS.
  For information about configuring the Nortel SNAS using the BBI, see *Nortel Secure Network Access Switch Configuration — Using the BBI* (NN47230-500).
- Enterprise Policy Manager (EPM) release 4.2
  Enterprise Policy Manager (EPM) is a security policy and quality of service provisioning application. You can use EPM to provision filters on the Nortel SNAS network access devices. EPM 4.2 supports preconfiguration of Red, Yellow, and Green VLAN filters prior to enabling the Nortel SNAS feature. In future releases of the Nortel SNAS and EPM software, users will have the additional ability to add and modify security and quality of service filters while Nortel SNAS is enabled on the device.
  For general information about installing and using EPM, see *Installing Nortel Enterprise Policy Manager (318389)*, .
- Simple Network Management Protocol (SNMP) agent
  For information about configuring SNMP for the Nortel SNAS, see "Configuring SNMP" (page 323).

Nortel SNAS configuration roadmap

The following task list is an overview of the steps required to configure the Nortel SNAS.

Step	Action
1	Configure the network DNS server to create a forward lookup zone for the Nortel SNAS domain. For an example, see "Configuration example" (page 385).
2	Configure the network DHCP server. For an example, see "Configuration example" (page 385). For each VLAN:

a Create a DHCP scope.

b Specify the IP address range and subnet mask for that scope.

c Configure the following DHCP options:

- Specify the default gateway.
- Specify the DNS server to be used by endpoints in that scope.
- If desired, configure DHCP so that the IP Phones learn their VLAN configuration data automatically from the DHCP server. For more information, see "Configuring DHCP to auto-configure IP Phones" (page 493).

ATTENTION
For the Red VLANs, the DNS server setting is one of the Nortel SNAS portal Virtual IP addresses (pVIP).

While the endpoint is in the Red VLAN, there are limited DNS server functions to be performed, and the Nortel SNAS itself acts as the DNS server. When the endpoint is in one of the other VLANs, DNS requests are forwarded to the corporate DNS servers.

The DNS server setting is required for the captive portal to work.

3 Configure the network core router:

a Create the Red, Yellow, Green, VoIP, and Nortel SNAS management VLANs.

b If the edge switches are operating in Layer 2 mode, enable 802.1q tagging on the uplink ports to enable them to participate in multiple VLANs, then add the ports to the applicable VLANs.

ATTENTION
The uplink ports must participate in all the VLANs.

c Configure IP addresses for the VLANs.

These IP interfaces are the default gateways the DHCP Relay will use.

d If the edge switches are operating in Layer 2 mode, configure DHCP relay agents for the Red, Yellow, Green, and VoIP VLANs.

Use the applicable show commands on the router to verify that DHCP relay is activated to reach the correct scope for each VLAN.

For more information about performing these general configuration steps, see the regular documentation for the type of router used in your network.

4 Configure the network access devices:

a Configure static routes to all the networks behind the core router.

b Configure the switch management VLAN, if necessary.

c Configure and enable SSH on the switch.

d Configure the Nortel SNAS portal Virtual IP address (pVIP)/subnet.

e Configure port tagging, if applicable.

For a Layer 2 switch, the uplink ports must be tagged to allow them to participate in multiple VLANs.

f Create the port-based VLANs.

These VLANs are configured as VoIP, Red, Yellow, and Green VLANs in step i and step j.

g Configure DHCP relay and IP routing if the switch is used in Layer 3 mode.

h (Optional) Configure the Red, Yellow, Green, and VoIP filters.

The filters are configured automatically as predefined defaults when you configure the Red, Yellow, and Green VLANs (step j). Configure the filters manually only if your particular system setup requires you to modify the default filters. You can modify the filters after Nortel SNAS is enabled.

i Configure the VoIP VLANs.

j Configure the Red, Yellow, and Green VLANs, associating each with the applicable filters.

k Configure the Nortel SNAS ports.

Identify switch ports as either uplink or dynamic. When you configure the uplink ports, you associate the Nortel SNAS VLANs with those ports. Clients are connected on the dynamic ports. You can configure Nortel SNAS ports (both dynamic and uplink) after Nortel SNAS is enabled globally.

l Enable Nortel SNAS globally.

For more information about configuring an Ethernet Routing Switch 5510, 5520, or 5530 in a Nortel SNAS network, see *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.1*, .

For more information about configuring an Ethernet Routing Switch 8300 in a Nortel SNAS network, see *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8* , .

For an example of the commands used to create a Nortel SNAS configuration, see “Configuration example” (page 385).

5 Perform the initial setup on the Nortel SNAS (see "Initial setup" (page 43)). Nortel recommends running the quick setup wizard during initial setup, in order to create and configure basic settings for a fully functional portal.

6 Enable SSH and SRS Admin to allow communication with the SREM (see "Configuring administrative settings" (page 281)).

7 Generate and activate the SSH key for communication between the Nortel SNAS and the network access devices (see "Managing SSH keys" (page 68)).

8 Specify the Software Requirement Set (SRS) rule for the default `nhauser` group (see "Configuring groups" (page 156)).

9 Add the network access devices and export the SSH key (see "Adding a network access devices " (page 60)).

10 Specify the VLAN mappings (see "Mapping the VLANs" (page 66)).

11 Test Nortel SNAS connectivity by using the **`/maint/chkcfg`** command (see "Performing maintenance" (page 353)).

12 Configure groups (see "Configuring groups and profiles" (page 149)).

13 Configure client filters (see "Configuring client filters" (page 162)).

14 Configure extended profiles (see "Configuring extended profiles" (page 164)).

15 Specify the authentication mechanisms (see "Configuring authentication" (page 171)).

16 Configure system users (see "Managing system users and groups" (page 211)).

17 Configure the end user experience (see "Customizing the portal and user logon" (page 227)).

--End--

Initial setup

This chapter includes the following topics:

Before you begin

Before you can set up the Nortel SNAS, you must complete the following tasks:

Step	Action
1	Plan the network. For more information, see *Nortel Secure Network Access Solution Guide*, (NN47230-200). In order to configure the Nortel SNAS, you require the following information: • IP addresses — Nortel SNAS Management IP address (MIP), portal Virtual IP address (pVIP), Real IP address (RIP) — default gateway — DNS server — NTP server (if applicable) — external authentication servers (if applicable)

- network access devices
- remediation server (if applicable)

For more information about the Nortel SNAS MIP, pVIP, and RIP, see "About the IP addresses" (page 42).

- VLAN IDs
  - Nortel SNAS management VLAN
  - Red VLANs
  - Yellow VLANs
  - Green VLANs
  - VoIP VLANs (optional)
- Groups and profiles to be configured

2 Configure the network DNS server, DHCP server, core router, and network access devices, as described in "Nortel SNAS configuration roadmap" (page 37), steps 1 through 4.

3 Install the Nortel SNAS device. For more information, see *Nortel Secure Network Access Switch 4050 Installation Guide* , (NN47230-300).

4 Establish a console connection to the Nortel SNAS (see "Establishing a console connection" (page 378)).

--End--

About the IP addresses

Management IP address

The Management IP address (MIP) identifies the Nortel SNAS in the network. In a multi-Nortel SNAS solution, the MIP is an IP alias to one of the Nortel SNAS devices in the cluster and identifies the cluster. The MIP always resides on a master Nortel SNAS device. If the master Nortel SNAS that currently holds the MIP fails, the MIP automatically migrates to a functional master Nortel SNAS. In order to configure the Nortel SNAS or Nortel SNAS cluster remotely, you connect to the MIP using Telnet (for the CLI) or SSH (for the CLI, the SREM or the BBI).

Portal Virtual IP address

The portal Virtual IP address (pVIP) is the address assigned to the Nortel SNAS device's web portal server. The pVIP is the address to which clients connect in order to access the Nortel SNAS network. While the client is in the Red VLAN and the Nortel SNAS is acting as DNS server, the pVIP is the DNS server IP address. Although it is possible to assign more than one pVIP to a Nortel SNAS device, Nortel recommends that each Nortel SNAS have only one pVIP. When the Nortel SNAS portal is configured as a captive portal, the pVIP is used to load balance logon requests.

Real IP address

The Real IP address (RIP) is the Nortel SNAS device host IP address for network connectivity. The RIP is the IP address used for communication between Nortel SNAS devices in a cluster. The RIP must be unique on the network and must be within the same subnet as the MIP.

ATTENTION
Nortel recommends that you always use the MIP for remote configuration, even though it is possible to configure the Nortel SNAS device remotely by connecting to its RIP. Connecting to the MIP allows you to access all the Nortel SNAS devices in a cluster. The MIP is always up, even if one of the Nortel SNAS devices is down and therefore not reachable at its RIP.

ATTENTION
If an IP address — MIP, VIP, RIP, or gateway — is changed, the Nortel SNAS must be rebooted for the change to take effect.

Initial setup

The initial setup is a guided process that launches automatically the first time you power up the Nortel SNAS and log on. You must use a console connection in order to perform the initial setup.

- For a standalone Nortel SNAS or the first Nortel SNAS in a cluster, see “Setting up a single Nortel SNAS device or the first in a cluster” (page 43).
- To add a Nortel SNAS to a cluster, see “Adding a Nortel SNAS device to a cluster” (page 50).

Setting up a single Nortel SNAS device or the first in a cluster

Step	Action

1	Log on using the following username and password:
	`login: admin`
	`Password: admin`
	The **Setup** Menu appears.

```
Alteon iSD NSNAS
Hardware platform:  4050
Software version:  x.x
-------------------------------------------------
----
[Setup Menu]
join - Join an existing cluster
new - Initialize host as a new installation
boot - Boot menu
info - Information menu
exit - Exit [global command, always available]
>> Setup#
```

2 Select the option for a new installation.

```
>> Setup# new

Setup will guide you through the initial configuration.
```

3 Specify the management interface port number. This port will be assigned to Interface 1.

```
Enter port number for the management interface [1-4]:
<port>
```

In an one-armed configuration, you are specifying the port you want to use for all network connectivity, since Interface 1 is used for both management traffic (Nortel SNAS management and connections to intranet resources) and client portal traffic (traffic between the Nortel Health Agent applet on the client and the portal).

4 Specify the RIP for this device. This IP address will be assigned to Interface 1.

```
Enter IP address for this machine (on management
interface): <IPaddr>
```

The RIP must be unique on the network and must be within the same subnet as the MIP.

5 Specify the network mask for the RIP on Interface 1.

```
Enter network mask [255.255.255.0]: <mask>
```

6 If the core router attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

```
Enter VLAN tag id (or zero for no VLAN) [0]:
```

If you do not specify a VLAN tag id (in other words, you accept the default value of zero), the traffic will not be VLAN tagged. When configuring the network access devices in Layer 2 configurations, ensure that you add the uplink ports to the Nortel

SNAS management VLAN, for traffic between the Nortel SNAS and the network access device.

7 Specify the default gateway IP address.

```
Enter default gateway IP address (or blank to skip):
<IPaddr>
```

The default gateway is the IP address of the interface on the core router that will be used if no other interface is specified. The default gateway IP address must be within the same network address range as the RIP.

8 Specify the MIP for this device or cluster.

```
Enter the Management IP (MIP) address: <IPaddr>
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

The MIP must be unique on the network and must be within the same subnet as the RIP and the default gateway for Interface 1.

WARNING

If you receive an error message that the iSD (the Nortel SNAS device) cannot contact the gateway, verify your settings on the core router. Do not proceed with the initial setup until the connectivity test succeeds.

9 Configure the interface for client portal traffic (Interface 2).

a Specify a port number for the client portal interface. This port will be assigned to Interface 2. The port number must not be the same as the port number for the management interface (Interface 1).

b Specify the RIP for Interface 2.

c Specify the network mask for the RIP on Interface 2.

d If the core router attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

e Specify the default gateway IP address for Interface 2. The default gateway is the IP address of the interface on the core router that will be used if no other interface is specified. The default gateway IP address on Interface 2 must be within the same subnet as the RIP for Interface 2.

```
Enter port number for the traffic interface [1-4]:
<port>
Enter IP address for this machine (on traffic
interface): <IPaddr>
Enter network mask [255.255.255.0]: <mask>
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic
interface): <IPaddr>
```

10 Specify the time zone.

```
Enter a timezone or 'select' [select]: <timezone>
```

If you do not know the time zone you need, press **<CR>** to access the selection menus:

```
Select a continent or ocean: <Continent or ocean by
number>
Select a country: <Country by number>
Select a region: <Region by number, if applicable>
Selected timezone: <Suggested timezone, based on your
selections>
```

11 Enter the current date settings.

```
Enter the current date (YYYY-MM-DD) [2008-03-10]:
```

12 Enter the current time settings.

```
Enter the current time (HH:MM:SS) [00:04:10]:
```

13 Specify the NTP server, if applicable.

```
Enter NTP server address (or blank to skip): <IPaddr>
```

ATTENTION
If you do not have access to an NTP server at this point, you can configure this item after the initial setup is completed. See "Configuring date and time settings" (page 274).

14 Specify the DNS server.

```
Enter DNS server address (or blank to skip): <IPaddr>
```

15 Generate the new SSH host keys for secure management and maintenance communication from and to Nortel SNAS devices.

```
Generate new SSH host keys (yes/no) [yes]:
This may take a few seconds...ok
```

If you do not generate the SSH host keys at this stage, generate them later when you configure the system (see "Configuring Nortel SNAS host SSH keys" (page 284)).

For communication between the Nortel SNAS and the network access devices, generate the SSH key after you have completed the initial setup (see “Managing SSH keys” (page 68)).

16 Change the admin user password, if desired.

```
Enter a password for the "admin" user:
Re-enter to confirm:
```

Make sure you remember the password you define for the admin user. You will need to provide the correct admin user password when logging in to the Nortel SNAS (or the Nortel SNAS cluster) for configuration purposes.

17 Run the Nortel SNAS quick setup wizard. This creates all the settings required to enable a fully functional portal, which you can customize later (see “Configuring the domain” (page 79)).

For information about the default settings created by the wizard, see “Settings created by the quick setup wizard” (page 49).

18 Start the quick setup wizard.

```
Run NSNAS quick setup wizard [yes]: yes
   Creating default networks under /cfg/doamin #/aaa/
   network
```

19 Specify the portal virtual IP address (pvip) of the Nortel SNAS device.

```
Enter NSNAS Portal Virtual IP address(pvip): <IPaddr>
```

20 Specify a name for the Nortel SNAS domain.

```
Enter NSNAS Domain name: <name>
```

21 Specify any domain names you wish to add to the DNS search list, as a convenience to clients. If the domain name is in the DNS search list, clients can use a shortened form of the domain name in the address fields on the Nortel SNAS portal.

```
Enter comma separated DNS search list
(eg company.com,intranet.company.com):
```

For example, if you entered `company.com` in the DNS search list, users can type **`nsnas`** to connect to `nsnas.company.com` from the portal page.

22 If you want to enable HTTP to HTTPS redirection, create a redirect server.

```
Create http to https redirect server [yes]:
```

23 Specify the action to be performed when an SRS rule check fails. The options are:

- `restricted`. The session remains intact, but access is restricted in accordance with the rights specified in the access rules for the group.
- `teardown`. The SSL session is torn down.

The default is `restricted`.

```
Use restricted (teardown/restricted) action for Nortel
Health Agent check failure?  [yes]:
```

24 Create the default user and group.

The action to be performed when the Nortel Health Agent check fails depends on your selection in step f.

```
Using 'restricted' action for Nortel Health Agent check
failure.
Setting up user account policies...
Create default user account [yes]:
User name: nha
User password: nha

Creating SRS rule 'srs-rule-test' for compliancy
check.
This rule check for the presence of the file
C:\tunnelguard\tg.txt

  Creating client filter 'nha_passed'.
  Creating client filter 'nha_failed'.
  Creating linkset 'nha_passed'.
  Creating linkset 'nha_failed'.
  Creating group 'nhauser' with secure access.
Associating group 'nhauser' with srs rule 'srs-rule-te
st'.
  Creating extended profile, full access when
nha_passed
Enter green vlan id [110]: <VID>
  Creating extended profile, remediation access when
nha_failed
Enter yellow vlan id [120]: <VID>
  Creating user 'nha' in group 'nhauser'.

Setting up system account policies...
Create default system account [yes]:
System account name: sys
System account password: sys
  Creating client filter 'nha_passed'.
Creating client filter 'nha_system_failed'.
Creating SRS rule 'srs-rule-syscred-test' for
compliancy check.
This rule check for the presence of the file
```

```
C:\tunnelguard\tg.txt
Creating linkset 'nha_system_passed'.
Creating linkset 'nha_system_failed'.
Creating group 'nhauser' with secure access.
Associating group 'nhasystem' with srs rule
'srs-rule-syscred-test'.
Creating extended profile, full access when
nha_system_passed
Enter system green vlan id [115]: <VID>
Creating extended profile, remediation access when
nha_system_failed
Enter yellow vlan id [120]: <VID>
Creating system account 'nha' in group 'nhasystem'.
Setting activation date to 2008 03 10 0:03.
Setting earliest push date to 2008 03 09 23:59.
Setting system credentials in group 'nhasystem'.
Would you like to enable the Nortel Desktop Agent?
[yes]:
Enabling Nortel Desktop Agent login on the captive
portal.
Enable secure web based configuration management
[yes]:
Enabling configuration management to https://192.168.
0.62:4443
Loading default radius dictionaries.  Initializing
system......ok
Setup successful.  Relogin to configure.
```

--End--

Settings created by the quick setup wizard

The quick setup wizard creates the following basic Nortel SNAS settings:

Step	Action
1	A Nortel SNAS domain (Doamin 1). A Nortel SNAS domain encompasses all switches, authentication servers, and remediation servers associated with the Nortel SNAS.
2	A virtual SSL server. A portal IP address, or pVIP, is assigned to the virtual SSL server. Clients connect to the pVIP in order to access the portal.
3	A test certificate is installed and mapped to the Nortel SNAS portal.
4	The authentication method is set to Local database.

5 One test user is configured. You were prompted to set a user name and password during the quick setup wizard (in this example, user name and password are both set to `nha`). The test user belongs to a group called `nhauser`. There are two profiles within the group: `nha_passed` and `nha_failed`. Each profile is associated with a client filter and a linkset. The profiles determine the VLAN to which the user is allocated. Table 3 "Extended profile details" (page 50) shows the extended profiles that have been created.

Table 3
Extended profile details

Index	Client filter name	VLAN ID	Linkset name
1	nha_failed	yellow	nha_failed
2	nha_passed	green	nha_passed

6 One or several domain names have been added to the DNS search list, depending on what you specified at the prompt in the quick setup wizard. This means that the client can enter a short name in the portal's various address fields (for example, `inside` instead of `inside.example.com` if `example.com` was added to the search list).

7 If you selected the option to enable http to https redirection, an HTTP server was created to redirect requests made with http to https, since the Nortel SNAS portal requires an SSL connection.

--End--

Adding a Nortel SNAS device to a cluster

After you have installed the first Nortel SNAS in a cluster (see "Setting up a single Nortel SNAS device or the first in a cluster" (page 43)), you can add another Nortel SNAS to the cluster by configuring the second Nortel SNAS setup to use the same MIP. When you set up the Nortel SNAS to join an existing cluster, the second Nortel SNAS gets most of its configuration from the existing Nortel SNAS device in the cluster. The amount of configuration you need to do at setup is minimal.

You can later modify settings for the cluster, the device, and the interfaces using the **`/cfg/sys/[host <host ID> /interface]`** commands.

Before you begin

Log on to the existing Nortel SNAS device to check the software version and system settings. Use the **`/boot/software/cur`** command to check the currently installed software version (for more information, see "Managing software for a Nortel SNAS device" (page 363)). Use the **`/cfg/sys/accesslist/list`** command to view settings for the Access List (for more information, see "Configuring the Access List" (page 273)).

Do not proceed with the join operation until the following requirements are met.

- Verify that the IP addresses you will assign to the new Nortel SNAS device conform to Nortel SNAS network requirements. For more information, see “About the IP addresses” (page 42) and “Interface configuration” (page 35).
- The Access List is updated, if necessary.
  The Access List is a system-wide list of IP addresses for hosts authorized to access the Nortel SNAS devices by Telnet and SSH. If the **`/info/sys`** command executed on the existing Nortel SNAS shows no items configured for the Access List, no action is required. However, if the Access List is not empty before the new Nortel SNAS joins the cluster, you must add to the Access List the cluster’s MIP, the existing Nortel SNAS RIP on Interface 1, and the new Nortel SNAS RIP on Interface 1. You must do this before you perform the join operation, or the devices will not be able to communicate with each other.
  For information about adding entries to the Access List, see “Configuring the Access List” (page 273).
- The existing Nortel SNAS and the new Nortel SNAS must run the same version of software. If the versions are different, decide which version you want to use and then do one of the following:
  - To change the version on the new NSNAS, download the desired software image and reinstall the software (see “Reinstalling the software” (page 372)).
  - To change the version on the existing Nortel SNAS, download the desired software image and upgrade the software on the existing cluster (see “Upgrading the Nortel SNAS ” (page 367)).

ATTENTION
Nortel recommends always using the most recent software version.

Joining a cluster

Step	Action

1	Log on using the following username and password:
	`login: admin`
	`Password: admin`
	The **Setup** Menu appears.

```
Alteon iSD NSNAS
Hardware platform:  4050
Software version:  x.x
-------------------------------------------------
----
[Setup Menu]
join - Join an existing cluster
new - Initialize host as a new installation
boot - Boot menu
info - Information menu
exit - Exit [global command, always available]
>> Setup#
```

2 Select the option to join an existing cluster.

```
>> Setup# join

Setup will guide you through the initial configuration.
```

3 Specify the management interface port number. This port will be assigned to Interface 1.

```
Enter port number for the management interface [1-4]:
<port>
```

In a one-armed configuration, you are specifying the port you want to use for all network connectivity, since Interface 1 is used for both management traffic (Nortel SNAS management and connections to intranet resources) and client portal traffic (traffic between the Nortel Health Agent applet on the client and the portal).

ATTENTION
For consistency, Nortel recommends that you specify the same port number for the management interface port on all Nortel SNAS devices in the cluster.

4 Specify the RIP for this device. This IP address will be assigned to Interface 1.

```
Enter IP address for this machine (on management
interface): <IPaddr>
```

The RIP must be unique on the network and must be within the same subnet as the MIP.

5 Specify the network mask for the RIP on Interface 1.

```
Enter network mask [255.255.255.0]: <mask>
```

6 If the core router attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

```
Enter VLAN tag id (or zero for no VLAN) [0]:
```

7 Configure the interface for client portal traffic (Interface 2).

a Specify a port number for the client portal interface. This port will be assigned to Interface 2. The port number must not be the same as the port number for the management interface (Interface 1).

b Specify the RIP for Interface 2.

c Specify the network mask for the RIP on Interface 2.

d If the core router attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

```
Enter port number for the traffic interface [1-4]:
<port>
Enter IP address for this machine (on traffic
interface): <IPaddr>
Enter network mask [255.255.255.0]: <mask>
Enter VLAN tag id (or zero for no VLAN) [0]:
```

8 Specify the MIP of the existing cluster.

```
The system is initialized by connecting to the
management server on an existing iSD, which must be
operational and initialized.
Enter the Management IP (MIP) address: <IPaddr>
```

9 Specify the default gateway IP address for Interface 2. The default gateway is the IP address of the interface on the core router that will be used if no other interface is specified. The default gateway IP address on Interface 2 must be within the same subnet as the RIP for Interface 2.

```
Enter default gateway IP address (on the traffic
interface): <IPaddr>
```

10 Provide the correct admin user password configured for the existing cluster.

```
Enter the existing admin user password: <password>
```

11 Wait while the setup utility finishes processing. When processing is complete, you will see `Setup successful`.

The new Nortel SNAS automatically picks up all other required configuration data from the existing Nortel SNAS in the cluster. After a short while, you receive the `login` prompt.

```
Setup successful.
login:
```

--End--

Next steps

Step	Action
1	To enable the SREM connection to the Nortel SNAS: **a** Use the **/cfg/sys/adm/ssh on** command to enable SSH access to the Nortel SNAS (for more information, see "Configuring administrative settings" (page 281)). **b** Use the **/cfg/sys/adm/srsadmin ena** command to enable SRS administration (for more information, see "Enabling TunnelGuard SRS administration" (page 284)). This is automatically enabled at the time of quick wizard as a part of configuration management enable.

ATTENTION
For greater security, you may want to restrict access to the Nortel SNAS to those machines specified in an Access List. In this case, ensure that you add an IP address for the BBI to the Access List. For more information about using the Access List to control Telnet and SSH access, see "Configuring the Access List" (page 273).

From this point on, you can configure the Nortel SNAS using either the CLI or the BBI.

2 To enable remote management using Telnet, use the **/cfg/sys/adm/telnet on** command to enable Telnet access to the Nortel SNAS (for more information, see "Configuring administrative settings" (page 281)).

3 To finish connecting the Nortel SNAS to the rest of the network, complete the following tasks:

a Generate and activate the SSH keys for communication between the Nortel SNAS and the network access devices (see "Managing SSH keys" (page 68)).

b Specify the SRS rule for the nhauser group (see "Configuring groups" (page 156)).

c Add the network access devices (see "Adding a network access devices " (page 60)).

d Specify the VLAN mappings (see "Mapping the VLANs" (page 66)).

e If you did not run the quick setup wizard during the initial setup, configure the following:

- Create the domain (see “Creating a domain” (page 83)).
- Create at least one group.
- Specify the VLANs to be used when the Nortel Health Agent check succeeds and when it fails (see “Configuring extended profiles” (page 164)).

4 Save the configuration (see “Applying and saving the configuration” (page 55)).

--End--

Applying and saving the configuration

You must enter explicit commands in order to make configuration changes permanent and in order to create a backup configuration file.

If you have not already done so after each sequence of configuration steps, confirm your changes using the **`apply`** command.

To view your configuration on the screen, for copy and paste into a text file, use the following command:

```
/cfg/dump
```

To save your configuration to a TFTP, FTP, SCP, or SFTP server, use the following command:

```
/cfg/ptcfg
```

For more information, see “Backing up or restoring the configuration” (page 356).

Managing the network access devices

This chapter includes the following topics:

Before you begin

In Trusted Computing Group (TCG) terminology, the edge switches in a Nortel SNAS function as the Policy Enforcement Point. In this document, the term *network access devices* is used to refer to the edge switch once it is configured for the Nortel SNAS network.

The following edge switches can function as network access devices in the Nortel SNAS:

- Ethernet Routing Switch 8300
- Ethernet Routing Switch 5510, 5520, and 5530

Before you can configure the edge switches as network access devices in the Nortel SNAS domain, you must complete the following:

- Create the domain, if applicable. If you ran the quick setup wizard during initial setup, Domain 1 is created. For more information about creating a domain, see “Configuring the domain” (page 79).
- Configure the edge switches for Nortel SNAS (see “Nortel SNAS configuration roadmap” (page 37), step 4). For detailed information about configuring the edge switches for Nortel SNAS, see *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8* , or *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.1*, .

For secure communication between the Nortel SNAS and the network access devices, each must have knowledge of the other’s public SSH key. After you have added the network access devices to the Nortel SNAS domain, you must exchange the necessary SSH keys (see “Managing SSH keys” (page 68)).

You require the following information for each network access devices:

- IP address of the switch
- VLAN names and VLAN IDs for the Red, Yellow, and Green VLANs
- the TCP port to be used for Nortel SNAS communication
- for Ethernet Routing Switch 8300 switches, a valid rwa user name

Managing network access devices

The Nortel SNAS starts communicating with the network access devices as soon as you enable the switch on the Nortel SNAS by using the **`/cfg/domain #/switch #/ena`** command.

You cannot configure the VLAN mappings for a network access devices in the Nortel SNAS domain if the switch is enabled. When you add a network access devices to the domain, it is disabled by default. Do not enable the network access devices until you have completed the configuration. To reconfigure the VLAN mappings for an existing network access devices, first disable it by using the **`/cfg/domain #/switch #/dis`** command.

Roadmap of domain switch commands

The following roadmap lists the CLI commands to configure the network access devices in a Nortel SNAS deployment. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`/cfg/domain #/switch <switch ID>`	
`/cfg/domain #/switch #/delete`	

Command	Parameter
/cfg/domain #/switch <switch ID>	name <name>
	type ERS8300|ERS5500
	ip <IPaddr>
	mgmtproto <sscp|sscplite>
	port <port>
	rvid <VLAN ID>
	reset
	ena
	dis
	delete
/cfg/domain #/vlan	add <name> <VLAN ID>
	del <index>
	list
/cfg/domain #/switch #/vlan	add <name> <VLAN ID>
	del <index>
	list
/cfg/domain #/sshkey	generate
	show
	export
/cfg/domain #/switch #/sshkey	import
	add
	del
	show
	export
	user <user>
/cfg/domain #/switch #/hlthchk	interval <interval>
	deadcnt <count>
	sq-int <interval>
/cfg/domain #/switch #/dis	
/cfg/domain #/switch #/ena	

Adding a network access devices

You can add a network access devices to the configuration in two ways. You must repeat the steps for each switch that you want to add to the domain configuration.

- “Using the quick switch setup wizard” (page 60)
- “Manually adding a switch” (page 62)

Using the quick switch setup wizard

To add a network access devices to the Nortel SNAS domain using the quick switch setup wizard, use the following command:

`/cfg/doamin #/quick`

You can later modify all settings created by the quick switch setup wizard (see “Configuring the network access devices ” (page 64)).

Step	Action
1	Launch the quick switch setup wizard. `>> Main# /cfg/domain #/quick`
2	Specify the IP address of the network access devices. `IP address of Switch: <IPaddr>`
3	Specify the SNMP profile of the network access devices. If the quick setup of your domain is not completed in this case most likely there is no SNMP profile to select. See “Configuring SNMP Profiles” (page 75) for more information. `SNMP profile:`

4	It searches for the SNMP settings for the switch.
	You will receive an error message and be prompted to use the sscp or sscplite.
	`Starting auto discovery.....`
	`Using default SNMP Profile for auto discovery.....`
	`.`
	`Error: Auto Discovery Failed !! Please check the SNMP settings in the Switch`
	`Do you want to use sscp or sscplite <sscp/sscplite> [sscp]:`

ATTENTION
Based on the discovery result, the wizard asks for switch ports, switch uplinks port (in case of sscplite switch) or NSNA communication port (in case of sscp switch).

5 Specify the VLAN ID of the Red VLAN, as configured on the network access devices. The network access devices in the domain can share a common Red VLAN or can each have a separate Red VLAN.

```
Red vlan id of Switch: <VLAN ID>
```

6 Specify the type of switch. Valid options are:

`ERS8300` (for an Ethernet Routing Switch 8300), `ERS5500` or `ERS55` (for an Ethernet Routing Switch 5510, 5520, or 5530), and ERS4500.

The default is `ERS8300`.

ATTENTION
The input is case sensitive.

```
Enter the type of the switch (ERS8300/ERS5500/ERS4500)
[ERS8300]:
```

7 Specify the TCP port for communication between the Nortel SNAS and the network access devices. The default is port 5000.

```
NSNA communication port[5000]:
```

8 The SSH fingerprint of the switch is automatically picked up if the switch is reachable. If the fingerprint is successfully retrieved, go to step 7.

If the fingerprint is not successfully retrieved, you will receive an error message and be prompted to add the SSH key.

```
Trying to retrieve fingerprint...failed.
Error:  "Failed to retrieve host key"
Do you want to add ssh key?  (yes/no) [no]:
```

Choose one of the following:

a To paste in a public key you have downloaded from the switch, enter **`Yes`**. Go to step 6.

b To continue adding the switch to the configuration without adding its public SSH key at this time, press **Enter** to accept the default value (`no`). After you have added the switch, add or import the SSH public key for the switch (see "Managing SSH keys for Nortel SNAS communication" (page 71)).

Go to step 7.

9 To add the switch public key:

a At the prompt to add the SSH key, enter **Yes**.

b When prompted, paste in the key from a text file, then press **Enter**.

c Enter an ellipsis (...) to signal the end of the key.

d To continue, go to step 7.

```
Do you want to add ssh key?  (yes/no) [no]: yes

Paste the key, press Enter to create a new line,
and then type "..." (without the quotation marks)
to terminate.
> 47.80.18.98 ssh-dss
AAAAB3NzaC1kc3MAAABRAJfEJJvYic9yOrejtZ88prdWdRWBF8Q
km9iJz3I6t6O1nzymt1Z1DVMXxCSb2InPcjq3o7WfPKa3VnUNUg
TpESrFlH7ooK+Zys8iEUbmJ3kpAAAAFQCUE/74fr6ACaxJpMcz0
TlWwahdzwAAAFEAgPWVrk0VOOXQmfLhutwaTrxltIDkJzOEIXPf
AIEpvDsvnlNkFE/i2vVdq/GTKmAghfN3BYjRIQT0PAwUKOS5gky
fLG9I5rKqJ/hFWJThR4YAAABQI9yJG5Q7q+2Pnk+tx1Kd44nCD6
/9j7L4RIkIEnrDbgsVxvMcsNdI+HLnN+vmBR5wd+vrW5Bq/ToMv
PspwI+WbV8TjycWeC7nk/Tg++X53hc=
> ...
```

10 Wait while the wizard completes processing to add the network access devices, then enter **Apply** to activate the changes. The system automatically assigns the lowest available switch ID to the network access devices.

The switch is disabled when it is first added to the configuration. Do not enable the switch until you have completed configuring the system. For more information, see “Configuring the network access devices ” (page 64).

```
Creating Switch 1
Use apply to activate the new Switch.

>> domain #
```

--End--

Manually adding a switch

To add a network access devices and configure it manually, use the following command:

/cfg/domain #/switch <switch ID>

where

switch ID is an integer in the range 1 to 255 that uniquely identifies the network access devices in the Nortel SNAS domain.

When you first add the network access devices, you are prompted to enter the following information:

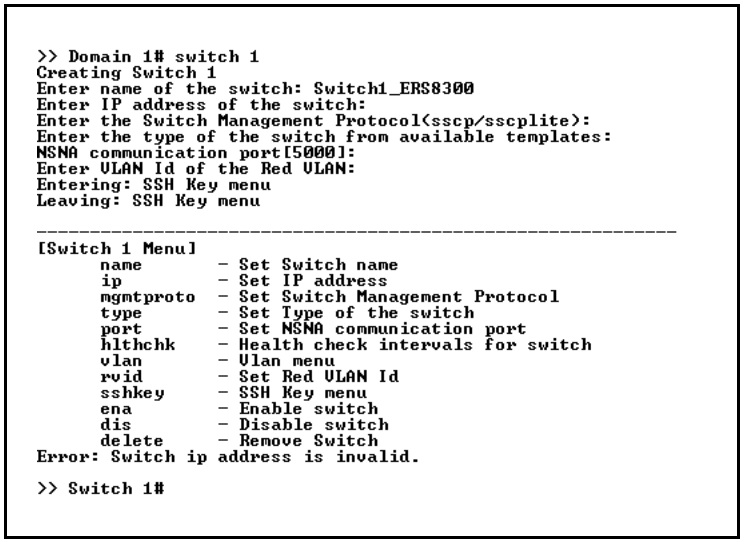
- switch name—a string that identifies the switch on the Nortel SNAS. The maximum length of the string is 255 characters. After you have defined a name for the switch, you can use either the switch name or the switch ID to access the **Switch** menu.
- type of switch—valid options are **`ERS8300`**, **`ERS5500`**, and **`ERS4500`**. The input is case sensitive.
- IP address of the switch.
- NSNA communication port—the TCP port for communication between the Nortel SNAS and the network access devices. The default is port 5000.
- Red VLAN ID—the VLAN ID of the Red VLAN configured on the switch.
- username—the user name for an rwa user on the switch (required for Ethernet Routing Switch 8300 only).

The SSH fingerprint of the switch is automatically picked up if the switch is reachable. If the fingerprint is not successfully retrieved, you receive an error message (`Error: Failed to retrieve host key`). After you have added the switch, you must add or import the SSH public key for the switch (see “Managing SSH keys for Nortel SNAS communication” (page 71)).

The **Switch** menu appears.

Figure 2 "Adding a switch manually" (page 64) shows sample output for the **`/cfg/domain #/switch`** command and commands on the **Switch** menu. For more information about the **Switch** menu commands, see “Configuring the network access devices ” (page 64).

Figure 2
Adding a switch manually



Deleting a network access devices

To remove a network access devices from the domain configuration, first disable the switch then delete it. Use the following commands:

`/cfg/domain #/switch #/dis`

`/cfg/domain/switch/delete`

The **`disable`** and **`delete`** commands log out all clients connected through the switch.

The **`delete`** command removes the current switch from the control of the Nortel SNAS cluster.

Configuring the network access devices

When you first add a network access devices to the Nortel SNAS domain, the switch is disabled by default. Do not enable the switch until you have completed configuring it. In particular, do not enable the switch until you have mapped the VLANs (see “Mapping the VLANs” (page 66)) and exchanged the necessary SSH keys (see “Managing SSH keys” (page 68)).

If you want to reconfigure the VLAN mappings or delete a VLAN for an existing network access devices, use the **`/cfg/domain/switch/dis`** command to disable the switch first.

ATTENTION
Remember to enable the network access devices after completing the configuration in order to activate the network access devices in the Nortel SNAS network.

To configure a network access devices in the Nortel SNAS domain, use the following command:

/cfg/domain #/switch <switch ID>

where

switch ID is the ID or name of the switch you want to configure.

The **Switch** menu appears.

The **Switch** menu includes the following options:

/cfg/domain #/switch <switch ID> **followed by:**	
name <name>	Names or renames the switch. After you have defined a name for the switch, you can use either the switch name or the switch ID to access the **Switch** menu. • **name** is a string that must be unique in the domain. The maximum length of the string is 255 characters.
type ERS8300 | ERS5500	Specifies the type of network access devices. Valid options are: • **ERS8300**—an Ethernet Routing Switch 8300 • **ERS5500**—an Ethernet Routing Switch 5510, 5520, or 5530 The default is **ERS8300**.
mgmtproto<mgmtproto>	Sets the Switch Management Protocol.
ip <IPaddr>	Specifies the IP address of the switch.
port <port>	Specifies the TCP port used for Nortel SNAS communication. The default is port 5000.
hlthchk	Accesses the **Healthcheck** menu, in order to configure settings for the Nortel SNAS to monitor the health of the switch (see "Monitoring switch health" (page 73)).
vlan	Accesses the **Switch Vlan** menu, in order to map the Green and Yellow VLANs configured on switch (see "Mapping the VLANs" (page 66)).

/cfg/domain #/switch <switch ID> **followed by:**	
rvid <VLAN ID>	Identifies the Red VLAN for the network access devices. • **VLAN ID** is the ID of the Red VLAN, as configured on the switch
sshkey	Accesses the **SSH Key** menu, in order to manage the exchange of public keys between the switch and the Nortel SNAS (see "Managing SSH keys for Nortel SNAS communication" (page 71))
reset	Resets all the Nortel SNAS -enabled ports on the switch. Clients connected to the ports are moved into the Red VLAN.
ena	Enables the network access devices. As soon as you enable the switch, the Nortel SNAS begins communicating with the switch and controlling its Nortel SNAS clients.
dis	Disables the switch for Nortel SNAS operation.
delete	Removes the switch from the Nortel SNAS domain configuration.

Mapping the VLANs

The VLANs are configured on the network access devices. You specify the Red VLAN for each network access devices when you add the switch (see "Adding a network access devices " (page 60)). After adding the switch, you must identify the Yellow and Green VLANs to the Nortel SNAS.

You can perform the VLAN mapping in two ways:

- for all switches in a domain (by using the **/cfg/domain #/vlan/add** command)
- switch by switch (by using the **/cfg/domain #/switch #/vlan/add** command)

Nortel recommends mapping the VLANs by domain. In this way, if you later add switches which use the same VLAN IDs, their VLAN mappings will automatically be picked up.

If you map the VLANs by domain, you can modify the mapping for a particular network access devices by using the switch-level **vlan** command. Switch-level settings override domain settings.

To manage the VLAN mappings for all the network access devices in the Nortel SNAS domain, first disable all the switches in the domain, then use the following command:

`/cfg/domain #/vlan`

To manage the VLAN mappings for a specific network access devices, first disable the switch in the domain, then use the following command:

`/cfg/domain #/switch #/vlan`

The Nortel SNAS maintains separate maps for the domain and the switch. If you add a VLAN from the domain-level **`vlan`** command, you must use the domain-level command for all future management of that mapping. Similarly, if you add a VLAN from the switch-level **`vlan`** command, you must use the switch-level command for all future management of that mapping.

The **Domain vlan** or **Switch vlan** menu appears.

The **Domain vlan** or **Switch vlan** menu includes the following options:

`/cfg/domain #[/switch #]/vlan` **followed by:**	
`add <name> <VLAN ID>`	Adds the specified VLAN to the domain or switch VLAN map. You are prompted to enter the required parameters if you do not include them in the command. • **`name`** is the name of the VLAN, as configured on the switch • **`VLAN ID`** is the ID of the VLAN, as configured on the switch The system automatically assigns an index number to the VLAN entry when you add it. If you are executing the command from the **Domain vlan** menu, the index number indicates the position of the new entry in the domain map. If you are executing the command from the **Switch vlan** menu, the index number indicates the position of the new entry in the switch map. Repeat this command for each Green and Yellow VLAN configured on the network access devices.

/cfg/domain #[/switch #]/vlan **followed by:**	
del <index>	Removes the specified VLAN entry from the applicable VLAN map. • **index** is an integer indicating the index number automatically assigned to the VLAN mapping when you created it The index numbers of the remaining entries adjust accordingly. To view the index numbers for all VLAN entries in the map, use the **/cfg/domain #[/switch #]/vlan/list** command.
list	The index number, name, and VLAN ID for all VLAN entries in the map.

Managing SSH keys

The Nortel SNAS and the network access devices controlled by the Nortel SNAS domain exchange public keys so that they can authenticate themselves to each other in future SSH communications.

To enable secure communication between the Nortel SNAS and the network access devices, do the following:

Step	Action
1	Generate an SSH public key for the Nortel SNAS domain (see "Generating SSH keys for the domain" (page 70)), if necessary. Apply the change immediately. If you created the domain manually, the SSH key was generated automatically (see "Manually creating a domain" (page 83)). **ATTENTION** The SSH key for the Nortel SNAS domain is not the same as the SSH key generated during initial setup for all Nortel SNAS hosts in the cluster (see "Initial setup" (page 41), step 15).
2	Export the Nortel SNAS public key to each network access devices. • For an Ethernet Routing Switch 8300: Use the **/cfg/domain #/switch #/sshkey/export** command to export the key directly to the switch (see

"Managing SSH keys for Nortel SNAS communication" (page 71)).

- For an Ethernet Routing Switch 5510, 5520, or 5530:
  Use the **/cfg/domain #/sshkey/export** command to upload the key to a TFTP server, for manual retrieval from the switch (see "Generating SSH keys for the domain" (page 70)). For information about downloading the key from the server to the switch, see *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.1*, .
  If you regenerate the key at any time, you must re-export the key to each network access devices.

  ATTENTION
  If you export the key after the network access devices are enabled, you may need to disable and re-enable the switch in order to activate the change.

3 For each network access devices, import its public key into the Nortel SNAS domain, if necessary (see "Managing SSH keys for Nortel SNAS communication" (page 71)).

- For an Ethernet Routing Switch 8300, you can retrieve the key in two ways:
  - Use the **/cfg/domain #/switch #/sshkey/import** command to import the key directly from the network access devices.
  - Use the **/cfg/domain #/switch #/sshkey/add** command to paste in the key.
- For an Ethernet Routing Switch 5510, 5520, or 5530:
  - Use the **/cfg/domain #/switch #/sshkey/import** command to import the key directly from the network access devices.

If the network access devices was reachable when you added it to the domain configuration, the SSH key was automatically retrieved.

If the network access devices defaults, it generates a new public key. You must reimport the key whenever the switch generates a new public key (see "Reimporting the network access devices SSH key" (page 72)).

ATTENTION
In general, enter **Apply** to apply the changes immediately after you execute any of the SSH commands.

--End--

Generating SSH keys for the domain

To generate, view, and export the public SSH key for the domain, use the following command:

`/cfg/domain #/sshkey`

The **NSNAS SSH key** menu appears.

The **NSNAS SSH key** menu includes the following options:

`/cfg/domain #/sshkey` **followed by:**	
`generate`	Generates an SSH public key for the domain. There can be only one key in effect for the Nortel SNAS domain at any one time. If a key already exists, you are prompted to confirm that you want to replace it. Enter **`Apply`** to apply the change immediately and create the key.
`show`	The SSH public key generated for the domain.
`export`	Exports the Nortel SNAS domain public key to a file exchange server. You are prompted to enter the following information: • protocol—options are `tftp|ftp|scp|sftp`. The default is `tftp`. **ATTENTION** Use TFTP to export to an Ethernet Routing Switch 5500 Series switch. Ethernet Routing Switch 5500 Series switches do not support the other protocols. • host name or IP address of the server • file name of the key (file type .pub) you are exporting • for FTP, SCP, and SFTP, user name and password to access the file exchange server To export the key directly to an Ethernet Routing Switch 8300, use the **`/cfg/domain #/switch #/sshkey/export`** command (see "Managing SSH keys for Nortel SNAS communication" (page 71)).

Figure 3 "Generating an SSH key for the domain" (page 71) shows sample output for the **/cfg/domain #/sshkey** command.

Figure 3
Generating an SSH key for the domain

```
>> Main# /cfg/domain 1/sshkey

------------------------------------------------------------
[NSNAS SSH key Menu]
   generate -Generate new SSH key for the NSNAS domain
   show     - Show NSNAS domain public SSH key

>> NSNAS SSH key# generate
Key already exists, overwrite? (yes/no) [no]: yes
Generating new SSH key, this operation takes a few sec-
onds... done.
Apply to activate.

>> NSNAS SSH key# apply
>> NSNAS SSH key# show

Type: DSA  Fingerprint:
4c:7c:b6:b4:47:5f:ae:6e:65:f1:b3:b1:7a:f0:59:d3
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBANWNQJzGnZ7lqIUZw5VkjseaR0dcgPhx/CA6Zl
JPZlRkY/USzJmZLoXpWuhAiByMPJ/69BLWCHTQUI/+FqNPzEXnjBBKHSw0
smb3OKfCJMfv4OfF7YQyfQP6KiKjsdNdHYH1ErHqNe1G8q8KIKin1G35z3
Bc7Yi9BxK84suWm3jdAAAAFQDg5ohEvhYoDlYhal3zMkgq0+t33wAAAIBh
Sa+J/5SxwYfnE/ltdwlOgcMk4eomP03M4BsI8vylsvHt4THD3typTtqjWo
jQG0vDBt7a/4hcHQ55LTrC81/u/+ep5NVlTjxlmczCz6C1wOq4Ab1iiQub
gRRL7DnZSghjNAU8JqzcEbU7g0VKorlxwt/M9P17ZmBdhkgwsdgArAAAAI
BtMdI1Q5eNq/yRmRuvinEwVjbQNVaywDkQljLvY4wnHjj+OjWpxVyLvzHI
Qs3IRBSzTCXGOqmmTNYXeDkHANPGl5RkfyldEq4/pJpUIMPBEj/C4H34Eq
WTkZvCaHRG3HH6QsJj3Wreskh574t/ubybhmzDw5Ubl42AxUJbDMVbZg==
---- END SSH2 PUBLIC KEY ----

>> NSNAS SSH key# export
Select protocol (tftp/ftp/scp/sftp) [tftp]:
Enter hostname or IP address of server: localhost
Enter filename on server: key.pub

Trying to export NSNAS public key to tftp://local-
host/key.pub

.
sent 590 bytes
>> NSNAS SSH key#
```

Managing SSH keys for Nortel SNAS communication

To retrieve the public key for the network access devices and export the public key for the domain, use the following command:

/cfg/domain #/switch #/sshkey

The **SSH Key** menu appears.

The **SSH Key** menu includes the following options:

/cfg/domain #/switch #/sshkey **followed by:**	
import	Retrieves the SSH public key from the network access devices, if it is reachable.
add	Allows you to paste in the contents of a key file you have downloaded from the Ethernet Routing Switch 8300 network access devices. When prompted, paste in the key, then press **Enter**. Enter an elllipsis (**...**) to signal the end of the key.
del	Deletes the SSH public key for the network access devices in the domain.
show	The SSH public key type and fingerprint for the network access devices.
export	Exports the SSH public key for the Nortel SNAS domain to the network access devices. **ATTENTION** You cannot use this command to export the key to an Ethernet Routing Switch 5500 series switch. Instead, use the **/cfg/domain#1/sshkey/export** command to upload the key to a file exchange server.
user <user>	Specifies the user name for the network access devices (required for Ethernet Routing Switch 8300 only). • **user** is the user name of an administrative user (rwa) on the switch.

Reimporting the network access devices SSH key

Whenever the network access devices generates a new public SSH key, you must import the new key into the Nortel SNAS domain.

Step	Action
1	Use the **/cfg/domain #/switch #/sshkey/del** command to delete the original key.
2	Enter **Apply** to apply the change immediately.
3	Use the **/cfg/domain #/switch #/sshkey/import** command to import the new key.
4	Enter **Apply** to apply the change immediately.

--End--

Monitoring switch health

The Nortel SNAS continually monitors the health of the network access devices. At specified intervals, a health check daemon sends queries and responses to the switch as a heartbeat mechanism. If no activity (heartbeat) is detected, the daemon will retry the health check for a specified number of times (the dead count). If there is still no heartbeat, then after a further interval (the status-quo interval) the network access devices moves all its clients into the Red VLAN. When connectivity is re-established, the Nortel SNAS synchronizes sessions with the network access devices.

The health check interval, dead count, and status-quo interval are configurable.

To configure the interval and dead count parameters for the Nortel SNAS health checks and status-quo mode, use the following command:

/cfg/domain #/switch #/hlthchk

The **HealthCheck** menu appears.

The **HealthCheck** menu includes the following options:

/cfg/domain #/switch #/hlthchk **followed by:**	
interval <interval>	Sets the time interval between checks for switch activity. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), or hours (h). The valid range is 60s (1m) to 64800s (18h). The default is 1m (1 minute).

/cfg/domain #/switch #/hlthchk **followed by:**	
deadcnt <count>	Specifies the number of times the Nortel SNAS will repeat the check for switch activity when no heartbeat is detected. • **count** is an integer in the range 1–65535 that indicates the number of retries. The default is 3. If no heartbeat is detected after the specified number of retries, the Nortel SNAS enters status-quo mode.
sq-int <interval>	Sets the time interval for status-quo mode, after which the network access devices moves all clients into the Red VLAN. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), or hours (h). The valid range is 0 to 64800s (18h). The default is 1m (1 minute).

Controlling communication with the network access devices

To stop communication between the Nortel SNAS and a network access devices, use the following command:

/cfg/domain #/switch #/dis

Enter **apply** to apply the change immediately.

ATTENTION
If the switch is not going to be used in the Nortel SNAS network, Nortel recommends deleting the switch from the Nortel SNAS domain, rather than just disabling it.

To restart communication between the Nortel SNAS and a network access devices, use the following command:

/cfg/domain #/switch #/ena

Enter **apply** to apply the change immediately.

Configuring SSCPLite

SSCPLite is a SNAS enforcement protocol that uses SNMP to restrict a users network access using dynamically provisioned VLAN's based on users credentials and device health assessment. SSCPLite supports

Nortel ES 325, 425, 450, 460, BPS, 470, and ERS 2500, 4500, 5500, 8300, and 8600. In addition, SSCPLite supports Cisco 2900, 3500, and 3700 series Ethernet switches.

- SSCPLite uses the SNMP Protocol
- Switches does not support Dynamic Host Control Protocol
- Switches may not support the DHCP signature based identification for VOIP phones
- Nortel SNAS should use MAC Authentication
- Multiple PCs connected using hub to the switch port are not supported.

To configure the sscplite, access the menu by using the following command.

cfg/domain #/switch #/mgmtproto

Configuration of switch menu are modified to include different communication protocols (sscp, sscplite). SSCP is selected by default.

Usage: mgmtproto <sscp/sscplite>

SSCP SSCPLite

The sscplite includes the following option:

/cfg/domain #/switch #/sscplite followed by:	
profile	Set SNMP profile to use

Configuring SNMP Profiles

To configure the snmp profiles, use the following command:

cfg/domain #/snmp-profile

Enter the SNMP profile number. Creates the SNMP profile #.
Enter the name of this SNMP profile.
Enter the version supported for the SNMP profile. Values are v1, v2c, and v3.
Enter the SNMP port to communicate.
Enter the data refresh interval in seconds.
Enter the CLI user name.
Enter the CLI user password.
Reconfirm the password.
Enter the CLI login type. Values are ssh and telnet.

The SNMPProfile # menu appears.

The snmp profile menu includes the following options:

/cfg/domain #/snmp-profile followed by	
<name>	Set the name of the profile.
<versions>	Set the supported SNMP versions.
<community>	SNMP community menu appears.
<port>	Set SNMP port to communicate.
refresh	Set the data refresh rate interval.
<cli-user>	Set the CLI login user name.
<cli-passwd>	Set the CLI login password.
<cli-logint>	Set the CLI login type.
del	Deletes the SNMP profile.

Configuring SNMP Versions

For configuring SNMP versions, use the following command:

/cfg/domain #/snmp-profile #/versions

The different versions of SNMP are the SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1 is the standard version of SNMP. SNMPv1 framework distinguishes between application entities and protocol entities.
- The SNMPv2c was created as an update of SNMPv1 with several features. The key enhancements of SNMPv2c are focused on the SMI, Manager-to-manager capability, and protocol operations.
- SNMPv3 defines the secure version of the SNMP. In SNMPv3, the concept of an authentication service is expanded to include other services, such as privacy. SNMPv3 also facilitates remote configuration of the SNMP entities. SNMPv3 was formed mainly to address the deficiencies related to security and administration.

Configuring SSCPLite Community

To configure SSCPLite Community, use the following command

/cfg/domain #/snmp-profile #/community

- SNMP community is the group that devices and manages stations running SNMP. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities.
- SNMP can be protected from the internet with a firewall. When a device receives an authentication that fails, a trap is sent to a management station.

The SSCPLite Community menu appears.

The SSCPLite Community menu includes the following options:

/cfg/domain #/snmp-profile #/community followed by:	
read	Set Read Community string **Read = Public**
write	Set Write Community string **Write = Private**
trap	Set Trap Community string. **trap = trap**

Configuring SNMP Templates

To configure the SNMP templates, use the following commands:

/cfg/device

The SNMP templates includes the following options:

/cfg/device followed by	
list	Lists the templates being used.
show	Shows the detailed information in the template.
import	Imports new switch Templates to the SNAS. This will add one more switch type in the domain Menu.

export	Export new switch Templates to the Tftp servers.
clear	Delete command will delete the template entry from the list and can delete the whole list of Templates.

Configuring the domain

This chapter includes the following topics:

A Nortel SNAS domain encompasses all the switches, authentication servers, and remediation servers associated with that Nortel SNAS cluster.

If you ran the quick setup wizard during initial setup, Domain 1 is created. If you did not run the quick setup wizard, you must create at least one domain. For information about creating a domain, see “Creating a domain” (page 83).

To delete a domain, see “Deleting a domain” (page 89).

ATTENTION
With Nortel Secure Network Access Switch Software Release 1.6.1, you cannot configure the Nortel SNAS to have more than one domain.

Configuring the domain

To configure the domain, access the **Domain** menu by using the following command:

/cfg/domain

From the **Domain** menu, you can configure and manage the following:

- domain parameters such as name and portal IP address (pVIP) (see "Configuring domain parameters" (page 89))
- Authentication, Authorization, and Accounting (AAA) features
  - for authentication, see "Configuring authentication" (page 171)
  - for authorization, see "Configuring groups and profiles" (page 149) and "Configuring the Nortel Health Agent check" (page 92)
  - for accounting, see "Configuring RADIUS accounting" (page 110)
- SNMP profile (see "Configuring SNMP Profiles" (page 75)
- PatchLink (see "Configuring Lumension PatchLink integration " (page 124))
- RADIUS server (see "Configuration of the RADIUS server" (page 127))
- NAP Interoperability (see "Configuration of Microsoft NAP Interoperability" (page 139))
- Location based security (see "Creation of the location" (page 123))
- the SSL server used for the domain portal (see "Configuring the SSL server" (page 97))
  - SSL trace commands
  - SSL settings
  - logging traffic with syslog messages
- portal settings (see "Customizing the portal and user logon" (page 227))
  - captive portal
  - portal look and feel
  - linksets
- the network access devices (see "Managing the network access devices " (page 57))
- the Nortel SNAS VLANs (see "Managing the network access devices " (page 57))
- SSH keys for the domain (see "Managing SSH keys" (page 68))
- HTTP redirect settings (see "Configuring HTTP redirect" (page 107))
- advanced settings such as a backend interface and logging options (see "Configuring advanced settings" (page 109))

Roadmap of domain commands

The following roadmap lists the CLI commands to configure the domain in a Nortel SNAS deployment. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
/cfg/domain <domain ID>	
/cfg/quick	
/cfg/domain #/del	
/cfg/domain <domain ID>	name <name>
	pvips <IPaddr>
/cfg/domain #/aaa/nha	recheck <interval>
	heartbeat <interval>
	hbretrycnt <count>
	hbretrycnt <count>
	status-quo on|off
	onflysrs on|off
	desktopnam Desktop agent shortcut name
	action teardown | restricted
	list
	details on|off
	custscript on|off
	persistoob on|off
	loglevel fatal | error | warning | info | debug
/cfg/domain #/aaa/nha/quick	
cfg/domain #/aaa/nha/desktopagent	Usage: desktopagent <on|off|auto>
/cfg/domain #/server	port <port>
	interface <interface ID>
	dnsname <name>
/cfg/domain #/server/trace	ssldump
	tcpdump
	ping <host>
	dnslookup <host>
	traceroute <host>

Command	Parameter
/cfg/domain #/server/ssl	cert <certificate index>
	cachesize <sessions>
	cachettl <ttl>
	cacerts <certificate index>
	cachain <certificate index list>
	protocol ssl2 | ssl3 | ssl23 | tls1
	ciphers <cipher list>
	ena
	dis
/cfg/domain #/server/adv/traflog	sysloghost <IPaddr>
	udpport <port>
	protocol ssl2 | ssl3 | ssl23 | tls1
	priority debug | info | notice
	facility auth | authpriv | daemon | local0-7
	ena
	dis
/cfg/domain #/httpredir	port <port>
	redir on | off
/cfg/domain #/adv	interface <interface ID>
	log
/cfg/domain #/aaa/radacct	ena
	dis
/cfg/domain #/aaa/radacct/servers	list <ip> <port> <secret>
	del <index number>
	add <ip> <port> <secret>
	insert <position> <ip> <port> <secret>
	move <index number value> <new index number value>
/cfg/domain #/aaa/radacct/domainattr	vendorid
	vendortype

Creating a domain

You can create a domain in two ways:

- “Manually creating a domain” (page 83)
- “Using the Nortel SNAS domain quick setup wizard in the CLI” (page 84)

Manually creating a domain

To create and configure a domain manually, use the following command:

/cfg/domain <domain ID>

where

domain ID is an integer in the range 1 to 256 that uniquely identifies the domain in the Nortel SNAS cluster.

When you first create the domain, you are prompted to enter the following parameters:

- domain name—a string that identifies the domain on the Nortel SNAS, as a mnemonic aid. The maximum length of the string is 255 characters.
- portal Virtual IP address (pVIP)—the IP address of the Nortel SNAS portal. You can have more than one pVIP for a domain. To specify more than one pVIP, use a comma separator. The pVIP is the address to which the client connects for authentication and host integrity check. For more information, see “About the IP addresses” (page 42).

The **Domain** menu appears.

Figure 4 "Creating a domain" (page 84) shows sample output for the **/cfg/domain <domain ID>** command and commands on the **Domain** menu. For more information about the **Domain** menu commands, see “Configuring domain parameters” (page 89).

Figure 4
Creating a domain

```
>> Main# /cfg/domain
Enter domain number (1-256): 2
Creating Domain 2
Domain name: MyDomain
Enter Domain Portal Vips(comma separated): 10.40.40.100
Entering: SSH key menu
Generating new SSH key, this operation takes a few
seconds... done.
Leaving: SSH key menu

------------------------------------------------------------
[Domain 2 Menu]
   name      - Set Domain name
   pvips     - Set Portal VIP addr(s) for the domain
   aaa       - AAA menu
   server    - SSL server menu
   portal    - Portal look and feel menu
   linkset   - Portal linkset menu
   switch    - Switch menu
   vlan      - Vlan menu
   sshkey    - SSH key menu
   dnscapt   - Dns captive portal menu
   httpredir- Http to Https redirection menu
   quick     - Quick switch setup wizard
   adv       - Advanced settings menu
   del       - Remove domain
Apply to activate.

>> Domain 2#
```

Using the Nortel SNAS domain quick setup wizard in the CLI

To create a domain using the Nortel SNAS quick setup wizard, use the following command:

`/cfg/quick`

The NSNAS quick setup wizard is similar to the quick setup wizard available during initial setup.

Depending on the options you select in connection with certificates and creating a test user, the two wizards also create similar default settings (see “Settings created by the quick setup wizard” (page 49)).

You can later modify all settings created by the domain quick setup wizard (see “Configuring domain parameters” (page 89)).

Step	Action
1	Launch the domain quick setup wizard. `>> Main# cfg/quick`
2	Specify the pVIP of the Nortel SNAS domain. You can configure additional pVIPs later (see "Configuring domain parameters" (page 89)). `IP address of domain portal: <IPaddr>`
3	Specify a name for the Nortel SNAS domain, as a mnemonic aid. `Name of the domain: <name>`
4	Specify the port on which the portal web server listens for SSL communications. The default for HTTPS communications is port 443. `Listen port of domain portal [443]:`
5	Specify the certificate to be used by the portal server. `Use existing certificate (no/1) [no]:` If certificates exist on the system, the certificate numbers will be offered as valid input options. Choose one of the following: **a** To create a new certificate by pasting in the contents of a certificate file from a text editor, press **Enter** to accept the default value (no). Go to step 6. **b** To create a test certificate, press **Enter** to accept the default value (no). Go to step 7. **c** To use an existing certificate, enter the applicable certificate number. Go to Step 8. Use the **/info/certs** command to view the main attributes of all configured certificates. The certificate number is shown in the Certificate Menu line (for example, `Certificate Menu 1:`). For more information about certificates and keys, see "Managing certificates" (page 297).
6	To create a new certificate: **a** At the prompt to create a test certificate, enter **No**. **b** When prompted, paste in the certificate and key from a text file, then press **Enter**. **c** Enter an ellipsis (...) to signal the end of the certificate. **d** To continue, go to Step 8.

```
Use existing certificate (no/1) [no]:
Create a test certificate?  (yes/no): no
Enter server certificate.

Paste the certificate and key, press Enter to create a
new line, and then type "..." (without the quotation
marks) to terminate.
>
```

7 To create a test certificate:

a At the prompt to create a test certificate, enter **Yes**.

b When prompted, enter the required certificate information. For more information, see "Generating and submitting a CSR" (page 305).

c To continue, go to Step 8.

```
Use existing certificate (no/1) [no]:
Create a test certificate?  (yes/no): yes
The combined length of the following parameters may not
exceed 225 bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (eg, city):
Organization Name (eg, company):
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname):
Email Address:
Subject alternative name (blank or comma separated
list of URI:<uri>, DNS:<fqdn>, IP:<ip-address>,
email:<email-address>):
Valid for days [365]:
Key size (512/1024/2048/4096) [1024]:
```

8 Specify whether the SSL server uses chain certificates.

```
Do you require chain certificates (yes/no) [no]:
```

9 If you want to enable HTTP to HTTPS redirection, create a redirect server.

```
Do you want an http to https redirect server (yes/no)
 [no]:
```

10 Specify whether you want to add a network access devices to the domain.

```
Do you want to configure a switch?  (yes/no) [no]:
```

If you do want to add a network access devices, enter **yes** to launch the quick switch wizard. Go to step 11.

If you do not want to add a network access devices at this time, press **Enter** to accept the default value (no). Go to step 12.

11 To add a network access devices, enter the required information when prompted. For more information, see "Using the quick switch setup wizard" (page 60).

```
Do you want to configure a switch? (yes/no) [no]: yes
Enter the type of the switch (ERS8300/ERS5500)
[ERS8300]: IP address of Switch:
NSNA communication port[5000]:
Red vlan id of Switch:
```

To continue, go to step 12.

12 Specify the action to be performed when an SRS rule check fails. The options are:

- restricted—the session remains intact, but access is restricted in accordance with the rights specified in the access rules for the group
- teardown—the SSL session is torn down

The default is restricted.

```
In the event that the Nortel health Agent checks fails
on a client, the session can be teardown, or left in
restricted mode with limited access.
Which action do you want to use for Health Agent check
failure? (teardown/restricted) [restricted]:
```

13 Specify whether you want to create a test local user (nha) in the default nhauser group.

```
Do you want to create a test local user? (yes/no)
[yes]:
```

If you do want to create a test user, press **Enter** to accept the default value (yes). The wizard will create a test user named nha, with password nha, in the default nhauser group.

If you do not want to create a test user, enter **no**.

14 Specify whether you want to create a test user for system authentication.

```
Do you want to create a test user for system
authentication? (yes/no) [yes]:
```

15 Wait while the wizard completes processing to create the domain, then enter **Apply** to activate the changes.

The wizard assigns the following default VLAN IDs:

- Green VLAN = VLAN ID 110
- Yellow VLAN = VLAN ID 120

You can change the VLAN mappings when you add or modify the network access devices (see “Configuring the network access devices ” (page 64)). You specify the Red VLAN when you add the network access devices to the domain.

The components created by the wizard depend on the selections you made in the preceding steps. For example, the sample output illustrates the following options:

- an existing certificate (Certificate 1) is being used
- no network access devices is being added
- the test user is being created

--End--

```
Creating Domain 1
Creating Certificate 1
Creating Client Filter 1
Name:  nha_passed
Creating Client Filter 2
Name:  nha_failed
Creating Client Filter 3
Name:  nha_system_passed
Creating Client Filter 4
Name:  nha_system_failed
Creating Linkset 1
Name:  nha_passed
This Linkset just prints the Health Agent result
Creating Linkset 2
Name:  nha_failed
This Linkset just prints the Health Agent result
Creating Linkset 3
Name:  nha_system_passed
This Linkset just prints the Health Agent result
Creating Linkset 4
Name:  nha_system_failed
This Linkset just prints the Health Agent result
```

```
Creating Group 1
Name:  nhauser
Creating Extended Profile 1
Giving full access when health check passed
Creating "green" vlan with id 110
Creating Access rule 1
Giving remediation access when health check failed
Creating Extended Profile 2
Not using SRS rule for user compliancy:
Creating Authentication 1
Adding user 'nha' with password 'nha'
Creating Group 2
```

```
Group for system policies
Name:  nhasystem
Creating Extended Profile 1
Giving system access when system health checks passed
Creating "green_system" vlan with id 115
Creating Extended Profile 2
Giving remediation access when system health checks failed
Creating "yellow" vlan with id 120
Not using SRS rule for system compliancy
2008 03 10 00:46
2008 03 10 00:14
Setting Activation and Earliest Push Date
Enable System Credentials
Adding user 'nhasystem' with password 'nhasystem' Use apply to
activate the new domain.
>> Configuration# apply
Changes applied successfully.
```

Deleting a domain

To delete a domain, use the following command:

/cfg/domain #/del

This command removes the current domain from the system configuration, including all settings in menus and submenus for the portal, groups, authentication services, linksets, and network access devices configured for that domain.

Configuring domain parameters

To configure the domain, use the following command:

/cfg/domain <domain ID>

where

domain ID is an integer in the range 1 to 256 that uniquely identifies the domain in the Nortel SNAS cluster.

The **Domain** menu appears.

The **Domain** menu includes the following options:

Table 4
Configuring domain parameters

/cfg/domain <domain ID> **followed by:**	
name<name>	Names or renames the domain. • **name** is a string that must be unique in the domain. The maximum length of the string is 255 characters. The name is a mnemonic aid only and is not used by other functions.
pvips <IPaddr>	Sets the pVIP for the domain. The pVIP is the portal address to which clients connect in order to access the Nortel SNAS network. For more information, see “About the IP addresses” (page 42). A domain can have more than one pVIP. To configure multiple IP addresses for the portal, use a comma to separate the IP address entries.
aaa	Accesses the **AAA** menu, in order to configure authentication, authorization, and accounting features. • For authentication, see “Configuring authentication” (page 171). • For authorization, see “Configuring groups and profiles” (page 149) and .“Configuring the Nortel Health Agent check” (page 92) • For accounting, see “Configuring RADIUS accounting” (page 110).
location	Accesses the **Location** menu for the location based security. (see “Creation of the location” (page 123))
patchlink	Accesses the **PatchLink Servers** menu. (see “Configuring Lumension PatchLink integration ” (page 124))
server	Accesses the **Server** menu, in order to configure the portal SSL server (see “Configuring the SSL server” (page 97)).

Table 4
Configuring domain parameters (cont'd.)

`/cfg/domain <domain ID>` **followed by:**	
`portal`	Accesses the **Portal** menu, in order to customize the portal page that in the client's web browser (see "Customizing the portal and user logon" (page 227)).
`linkset`	Accesses the **Linkset** menu, in order to configure the linksets to display on the portal Home tab (see "Configuring linksets" (page 251)).
`switch`	Accesses the **Switch** menu, in order to configure the network access devices controlled by the Nortel SNAS domain (see "Managing network access devices " (page 58)).
`snmp-profi`	Accesses the **SNMPProfile** menu. (see"Configuring SNMP Profiles" (page 75))
`vlan`	Accesses the **Domain vlan** menu, in order to manage VLAN mappings on the Nortel SNAS domain (see "Mapping the VLANs" (page 66)).
`dhcp`	Accesses the **DHCP** menu.
`sshkey`	Accesses the **NSNAS SSH key** menu, in order to generate and show the public SSH key for the Nortel SNAS domain (see "Generating SSH keys for the domain" (page 70)).
`dnscapt`	Accesses the **DNS capture** menu, in order to set the Nortel SNAS domain portal as a captive portal and to configure the Exclude List (see "Configuring the captive portal" (page 240)).
`httpredir`	Accesses the **HTTP Redir** menu, in order to configure HTTP to HTTPS redirect settings (see "Configuring HTTP redirect" (page 107)).
`radius`	Accesses the **RADIUS** menu to configure RADIUS server. (see"Configuration of the RADIUS server" (page 127))

Table 4
Configuring domain parameters (cont'd.)

`/cfg/domain <domain ID>` **followed by:**	
`nap`	Accesses the **NAP** menu to configure the NAP. (see"Configuration of Microsoft NAP Interoperability" (page 139))
`quick`	Launches the quick switch setup wizard, in order to add network access devices to the Nortel SNAS domain (see "Using the quick switch setup wizard" (page 60)).
`syslog`	Accesses the **Syslog Servers** menu.
`adv`	Accesses the **Advanced** menu, in order to configure a backend interface for the Nortel SNAS domain and specify the log settings for syslog messages (see "Configuring advanced settings" (page 109)).
`del`	Removes the current domain from the system configuration, including all settings in menus and submenus.

Configuring the Nortel Health Agent check

Before an authenticated client is allowed into the network, the Nortel Health Agent application checks client host integrity by verifying that the components required for the client's personal firewall (executables, DLLs, configuration files, and so on) are installed and active on the client PC. For more information about how the Nortel Health Agent check operates in the Nortel SNAS, see "Nortel Health Agent host integrity check" (page 32).

If you ran the quick setup wizard during the initial setup or to create the domain, the Nortel Health Agent check has been configured with default settings and the check result you selected (teardown or restricted). You can rerun the Nortel Health Agent portion of the quick setup wizard at any time by using the **`/cfg/domain #/aaa/nha/quick`** command (see "Using the quick Nortel Health Agent setup wizard in the CLI" (page 96)).

To configure settings for the Nortel Health Agent host integrity check and the check result, use the following command:

`/cfg/domain #/aaa/nha`

The **Nortel Health Agent** menu appears.

The **Nortel Health Agent** menu includes the following options:

Table 5
Configuring the Nortel Health Agent

/cfg/domain #/aaa/nha **followed by:**	
quick	Launches the Quick Nortel Health Agent setup wizard, in order to configure default Nortel Health Agent check settings and the check result (see “Using the quick Nortel Health Agent setup wizard in the CLI” (page 96)).
recheck <interval>	Sets the time interval between SRS rule rechecks made by the Nortel Health Agent applet on the client machine. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), hours (h), or days (d). The valid range is 60s (1m) to 86400s (1d). The default is 15m (15 minutes). If a recheck fails, the Nortel SNAS performs the action specified in the **action** command (see "action teardown|restricted" (page 94)).
heartbeat <interval>	Sets the time interval between checks for client activity. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), hours (h), or days (d). The valid range is 60s (1m) to 86400s (1d). The default is 1m (1 minute).
hbretrycnt <count>	Specifies the number of times the Nortel SNAS repeats the check for client activity when no heartbeat is detected. • **count** is an integer in the range 1–65535 that indicates the number of retries. The default is 3. If no heartbeat is detected after the specified number of retries (the inactivity interval), the Nortel SNAS default behavior is to terminate the session (see **/cfg/domain #/aaa/nha/status-quo**).

Table 5
Configuring the Nortel Health Agent (cont'd.)

/cfg/domain #/aaa/nha **followed by:**	
status-quo on|off	Specifies whether the Nortel SNAS domain operates in status-quo mode. Status-quo mode determines the behavior of the Nortel SNAS if no client activity is detected after the inactivity interval (`heartbeat x hbretrycnt`). The options are: • **on**—the client session continues indefinitely • **off**—the Nortel SNAS terminates the session immediately The default is **off**.
onflysrs	Enables or disables the on-the-fly-srs-update-mode. When a security policy is modified on the SNAS using the administrative tool the policy is updated on the Nortel Health Agent running on the logged in operating systems. Values: on and off default: off
desktopage	Enables or disables the desktop agent name. Values: on, off, and auto default: off
desktopnam	Specifies the desktop agent shortcut name.
action teardown|restricted	Specifies the action to be performed if the client fails the Nortel Health Agent SRS rule check. The options are: • **restricted**—the session remains intact, but access is restricted in accordance with the rights specified in the access rules for the group • **teardown**—the SSL session is torn down

Table 5
Configuring the Nortel Health Agent (cont'd.)

/cfg/domain #/aaa/nha **followed by:**	
list	Lists the SRS rules configured for the domain. For information about creating SRS rules, see the information about the Nortel Health Agent SRS Rule Builder in *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, . The Nortel Health Agent applet can apply different SRS rules for different groups. For information about specifying the SRS rule to use for the Nortel Health Agent, see "Configuring groups" (page 156).
details on|off	Specifies whether SRS failure details can be displayed on the portal page. Valid options are: • **on**—details will be displayed • **off**—details will not be displayed The default is **off**. If set to **on**, the client can click on the Nortel Health Agent icon on the portal page to display details about which elements of the SRS rule check failed.
custscript	Allows the client script customization. Values: on and off
persistoob	Persists the out-of-bound connections. Values: on and off
loglevel fatal|error|warning| info|debug	Sets the log level for the Nortel Health Agent applet. The options are: • **fatal**—fatal errors only • **error**—all errors • **warning**—warning information about conditions that are not error conditions

Table 5
Configuring the Nortel Health Agent (cont'd.)

/cfg/domain #/aaa/nha **followed by:**	
	• **info**—high-level information about processes • **debug**—detailed information about all processes The default is **info**. The information in the client's Java Console window. You can use the information to track errors in the Nortel Health Agent SRS rules.

Using the quick Nortel Health Agent setup wizard in the CLI

To configure the settings for the SRS rule check using the Nortel Health Agent quick setup wizard, use the following command:

/cfg/domain #/aaa/nha/quick

The Nortel Health Agent quick setup wizard is similar to the last few steps of the Nortel SNAS domain quick setup wizard. The wizard prompts you for the following information:

- the action to be performed if the Nortel Health Agent check fails (see step 12)
- whether you want to create a test user (see step 13)

The Nortel Health Agent quick setup wizard creates a default SRS rule (**srs-rule-test**). This rule checks for the presence of a text file on the client's machine (**C:\tunnelguard\tg.txt**).

The following table shows the sample output for the Nortel Health Agent quick setup wizard.

```
>> Main# /cfg/domain #/aaa/nha/quick
In the event that the Nortel Health Agent checks fails on a client, the session
can be teardown, or left in restricted mode with limited access.
Which action do you want to use for Nortel Health Agent check failure?
(teardown/restricted) [restricted]:
Do you want to create a test user for system authentication?  (yes/no) [yes]:
Do you want to create a test local user?  (yes/no) [yes]:

User policy configuration...
Creating Client Filter 1
```

```
Name:  nha_passed
Creating Client Filter 2
Name:  nha_failed
Using existing nha_passed linkset
Using existing nha_failed linkset
Using existing SRS Rule srs-rule-test
Creating Group 1
Group for user policies
Name:  nhauser
Creating Extended Profile 1
Giving full access when health check passed
Using existing green vlan
Creating Extended Profile 2
Giving remediation access when health check failed
Using existing yellow vlan
Using SRS rule for user compliancy:  srs-rule-test
Adding user 'nha' with password 'nha'

System policy configuration...
Creating Client Filter 3
Name:  nha_system_passed
Creating Client Filter 4
Name:  nha_system_failed
Using existing nha_system_passed linkset
Using existing nha_system_failed linkset
Using existing SRS Rule srs-rule-syscred-test
Creating Group 2
Group for system policies
Name:  nhasystem
Creating Extended Profile 1
Giving system access when system health passed
Using existing green_system vlan
Creating Extended Profile 2
Giving remediation access when system health failed
Using existing yellow vlan
Using SRS rule for system compliancy:  srs-rule-syscred-test
2008 03 10 00:50
2008 03 10 00:18
Setting Activation and Earliest Push Date
Enable System Credentials
Adding system account 'sys' with password 'sys'
Use 'diff' to view pending changes, and 'apply' to commit

>> Nortel Health Agent# apply Changes applied successfully.
```

Configuring the SSL server

The server number assigned to the portal server configured for the domain is server 1001.

To configure the portal server used in the domain, use the following command:

/cfg/domain #/server

The **Server 1001** menu appears.

The **Server 1001** menu includes the following options:

Table 6
Configuring SSL server

/cfg/domain #/server **followed by:**	
port <port>	Specifies the port to which the portal server listens for HTTPS communications. • **port** is an integer in the range 1–65534 that indicates the TCP port number. The default is 443.
interface <interface ID>	Specifies the backend interface used by the server. • **interface ID** is an integer that indicates the interface number. The default is 0.
dnsname <name>	Assigns a DNS name to the portal IP address. • **name** is the fully qualified domain name (FQDN) of the pVIP (for example, nsnas.example.com). Generally, you need to specify a DNS name only if your corporate DNS server is unable to perform reverse lookups of the portal IP address. When you press **Enter** after specifying the DNS name, the system performs a check against the DNS server included in the system configuration (see **/cfg/sys/dns**) to verify that: • the FQDN is registered in DNS • the resolved IP address corresponds to the pVIP
trace	Accesses the **Trace** menu, in order to capture and analyze SSL and TCP traffic between clients and the portal server. For more information, see "Tracing SSL traffic" (page 99).

Table 6
Configuring SSL server (cont'd.)

/cfg/domain #/server followed by:	
ssl	Accesses the **SSL Settings** menu, in order to configure SSL settings for the portal server (see "Configuring SSL settings" (page 102)).
adv	Accesses the **Advance settings** menu, in order to configure traffic log settings for a syslog server (see "Configuring traffic log settings" (page 105)).

Tracing SSL traffic

To verify connectivity and to capture information about SSL and TCP traffic between clients and the portal server, use the following command:

```
/cfg/domain #/server/trace
```

The **Trace** menu appears.

The **Trace** menu includes the following options:

Table 7
Tracing SSL traffic

/cfg/domain #/server/trace followed by:	
ssldump	Creates a dump of the SSL traffic flowing between clients and the portal server. You are prompted to enter the following information: • **ssldump flags** and **ssldump filter**—for more information about the flags and filter expressions available for SSLDUMP using UNIX, see http://www.tcpdump.org/tcpdump_man.html. • **output mode** Options for the output mode are: • **interactive**—captured information decrypted on the screen. SSLDUMP cannot decrypt any traffic if it is started after the browser. SSLDUMP must be running during the initial SSL handshake. • **tftp | ftp | sftp**—the dump will be saved as a file to the file exchange server you specify, using a destination file name you

/cfg/domain #/server/trace **followed by:**	
	specify. You are prompted to enter the required information. You can specify the file exchange server using either the host name or the IP address. For TFTP, the number of files sent depends on the amount of captured information. A sequence number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. For **ftp** and **sftp**, you will also be prompted to specify a user name and password valid on the file exchange server. The default output mode is **interactive**.
tcpdump	Creates a dump of the TCP traffic flowing between clients and the virtual SSL server. You are prompted to enter the following information: • **tcpdump flags** and **tcpdump filter**—for more information about the flags and filter expressions available for TCPDUMP using UNIX, see http://www.tcpdump.org/tcpdump_man.html. • **output mode** Options for the output mode are: • **interactive**—captured information on the screen • **tftp** | **ftp** | **sftp**—the dump will be saved as a file to the file exchange server you specify, using a destination file name you specify. You are prompted to enter the required information. You can specify the file exchange server using either the host name or the IP address. For TFTP, the number of files sent depends on the amount of captured information. A sequence number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. For **ftp** and **sftp**, you will also be prompted to specify a user name and password valid on the file exchange server.

/cfg/domain #/server/trace **followed by:**	
	You can read a saved TCP traffic dump file using the TCPDUMP or Ethereal application on a remote machine. The default output mode is **interactive**.
ping <host>	Verifies station-to-station connectivity across the network. • **host** is the host name or IP address of the target station If a backend interface is mapped to the current Nortel SNAS domain, the check is made through the backend interface. To map a backend interface to the domain, use the **/cfg/domain #/adv/interface** command (see "Configuring advanced settings" (page 109)). To be able to use a host name, the DNS parameters must be configured (see "Configuring DNS servers and settings" (page 276)).
dnslookup <host>	Finds the IP address for a machine whose host name you specify, or the host name of a machine whose IP address you specify. • **host** is the host name or IP address of the machine If a backend interface is mapped to the current Nortel SNAS domain, the check is made through the backend interface. To map a backend interface to the domain, use the **/cfg/domain #/adv/interface** command (see "Configuring advanced settings" (page 109)).
traceroute <host>	Identifies the route used for station-to-station connectivity across the network.

/cfg/domain #/server/trace followed by:	
	• **host** is the host name or IP address of the target station If a backend interface is mapped to the current Nortel SNAS domain, the check is made through the backend interface. To map a backend interface to the domain, use the **/cfg/domain #/adv/interface** command (see "Configuring advanced settings" (page 109)). To be able to use a host name, the DNS parameters must be configured (see "Configuring DNS servers and settings" (page 276)).

Configuring SSL settings

To configure SSL-specific settings for the portal server, use the following command:

/cfg/domain #/server/ssl

The **SSL Settings** menu appears.

The **SSL Settings** menu includes the following options:

Table 8
Configuring SSL Settings

/cfg/domain #/server/ssl followed by:	
cert <certificate index>	Specifies which server certificate the portal server will use. You cannot specify more than one server certificate for the server to use at any one time. • **certificate index** is an integer indicating the index number automatically assigned to the certificate when you created it To view basic information about available certificates, use the **/info/certs** command. For information about adding a new certificate, see "Installing certificates and keys" (page 299).

Table 8
Configuring SSL Settings (cont'd.)

/cfg/domain #/server/ssl **followed by:**	
cachesize <sessions>	Sets the size of the SSL cache. • **sessions** is an integer less than or equal to 10000 indicating the number of cached sessions. The default is 4000. If there are many cache misses, increase the **cachesize** value for better performance.
cachettl <ttl>	Specifies the maximum time to live (TTL) value for items in the SSL cache. After the TTL has expired, the items are discarded. • **ttl** is an integer that indicates the TTL value in seconds (s), minutes (m), hours (h), or days (d). If you do not specify a measurement unit, seconds is assumed. The default is 5m (5 minutes).
cacerts <certificate index>	Specifies which of the available CA certificates to use for client authentication. Not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
cachain <certificate index list>	Specifies the CA certificate chain of the server certificate. • **certificate index list** is a comma-separated list of the certificate index numbers assigned to the certificates in the chain. The chain starts with the issuing CA certificate of the server certificate and can range up to the root CA certificate. The command explicitly constructs the server certificate chain. The chain and the server certificate are sent to the browser. To clear all specified chain certificates, press **Enter** at the prompt to enter the certificate numbers. At the prompt to confirm that you want to clear the list, enter **yes**. **ATTENTION**

Table 8
Configuring SSL Settings (cont'd.)

/cfg/domain #/server/ssl **followed by:**	
	The SSL server can use chain certificates only if the protocol version is set to ssl3 or ssl23 (see **/cfg/domain #/server/ssl/protocol**).
protocol ssl2 | ssl3 | ssl23 | tls1	Specifies the protocol to use when establishing an SSL session with a client. Valid options are: • **ssl2**—accept SSL 2.0 only • **ssl3**—accept SSL 3.0 and TLS 1.0 • **ssl23**—accept SSL 2.0, SSL 3.0, and TLS 1.0 • **tls1**—accept TLS 1.0 only The default value is **ssl3**.
verify none | optional | required	Specifies the level of client authentication to use when establishing an SSL session. Valid options are: • **none**—no client certificate is required • **optional**—a client certificate is requested, but the client need not present one • **required**—a client certificate is required The default value is **none**. Not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
ciphers <cipher list>	Specifies the list of preferred ciphers. This information is sent to the backend servers.The default cipher list provides for using lighter encryption algorithms between the SNAS and the backend servers. Both the SNAS and the backend servers typically are behind a firewall in physically secured premises, using lighter encryption algorithms on this network segment should not compromise the overall security. If you change the default list of preferred ciphers, make sure the specified ciphers are

Table 8
Configuring SSL Settings (cont'd.)

/cfg/domain #/server/ssl **followed by:**	
	included in the backend servers' list of preferred ciphers as the SSL connection will otherwise be refused. Specifies the cipher preference list. • **cipher list** is an expression that consists of cipher strings separated by colons. The default cipher list is **ALL@STRENGTH**. For more information about cipher lists, see "Supported ciphers" (page 483).
ena **[<bool>]**	Enables SSL on the portal server. SSL is enabled by default.
dis **[<bool>]**	Disables SSL on the portal server. SSL is enabled by default.

Configuring traffic log settings

You can configure a syslog server to receive User Datagram Protocol (UDP) syslog messages for all HTTP requests handled by the portal server.

Nortel does not recommend routinely enabling this functionality for the following reasons:

- Logging traffic with syslog messages generates a substantial amount of network traffic.
- Logging traffic places an additional CPU load on each Nortel SNAS device in the cluster.
- In general, syslog servers are not intended for the traffic type of log message. Therefore, the syslog server might not be able to cope with the quantity of syslog messages generated within a cluster of Nortel SNAS devices.

Enable traffic logging with syslog messages in environments where laws or regulations require traffic logging to be performed on the SSL terminating device itself. You can also enable it temporarily for debugging purposes.

Because of the amount of traffic generated, Nortel recommends that you set up syslog on the backend server if possible.

A syslog message generated on a Nortel SNAS device looks like the following:

```
Mar 8 14:14:33 192.168.128.24 <ISD-SSL>:
192.168.128.189 TLSv1/SSLv3 DES-CBC3-SHA "GET / HTTP/1.0".
```

To set up a syslog server to receive UDP syslog messages for all HTTP requests handled by the portal server, use the following command:

`/cfg/domain #/server/adv/traflog`

The **Traffic Log Settings** menu appears.

The **Traffic Log Settings** menu includes the following options:

`/cfg/domain #/server/adv/traflog` **followed by:**	
`sysloghost <IPaddr>`	Specifies the IP address of the syslog server.
`udpport <port>`	Specifies the UDP port number of the syslog server. • **`port`** is an integer in the range 1–65534 that indicates the UDP port number. The default is 514.
`priority debug|info|notice`	Specifies the priority level of the syslog messages that are sent. Valid options are: • **`debug`**—information useful for debugging purposes only • **`info`**—informational messages • **`notice`**—information about conditions that are not error conditions but nevertheless warrant special attention The default value is **`info`**.

/cfg/domain #/httpredir followed by:	
ena	Enables traffic logging with syslog messages to the specified syslog server. Traffic logging with syslog messages is disabled by default.
dis	Disables traffic logging with syslog messages. Traffic logging with syslog messages is disabled by default.

Configuring HTTP redirect

You can configure the Nortel SNAS domain to automatically redirect HTTP requests to the HTTPS server. For example, a client request directed to `http://nsnas.com` is automatically redirected to `https://nsnas.com`.

To configure the domain to automatically redirect HTTP requests to the HTTPS server specified for the domain, use the following command:

`/cfg/domain #/httpredir`

The **Http Redir** menu appears.

The **Http Redir** menu includes the following options:

Table 9
Configuring HTTP redirect

/cfg/domain #/httpredir followed by:	
port <port>	Specifies the port to which the portal server listens for HTTP communications. • **port** is an integer that indicates the TCP port number. The default is 80. **ATTENTION** If you do not accept the default value and you specify a different port, you must modify the Red and Yellow filters on the network access devices accordingly.

	Otherwise, the client PC will not be able to reach the portal for user authentication.
redir on|off	Specifies whether HTTP requests will be redirected to the HTTPS server. • **on**—HTTP redirect is enabled • **off**—HTTP redirect is disabled The default is **off**.

Browser-Based Management Configuration

The HTTP menu is used for enabling/disabling browser-based configuration of your VPN Gateway. To access the Browser-Based Interface (BBI), enter the Management IP address assigned to SNAS cluster in your web browser.

The HTTP menu includes the following options:

Table 10
Browser-Based Management Configuration

cfg/sys/adm/http/ followed by	
port	Sets the port number to be used for browser-based SNAS configuration using the BBI.
ena	Enables the HTTP server used for browser-based configuration on the SNAS.
dis	Disables the HTTP server used for browser-based configuration on the SNAS.

Browser-Based Management Configuration with SSL

The HTTPS menu is used for enabling/disabling browser-based configuration of your VPN Gateway through a secure SSL tunnel. To access the Browser-Based Management Interface (BBI), enter the Management IP address assigned to your SNAS cluster in your web browser.

The HTTPS menu includes the following options

Table 11
Browser-Based Management Configuration with SSL

cfg/sys/adm/https followed by	
port	Sets the port number to be used for browser-based SNAS configuration from the BBI using SSL.
ena	Enables the HTTPS server used for browser-based configuration on the SNAS using SSL.
dis	Disables the HTTPS server used for browser-based configuration on the SNAS using SSL.

Configuring advanced settings

You can configure the following advanced settings for the Nortel SNAS domain:

- a backend interface
- logging options

To map a backend interface to the domain and to configure logging options, use the following command:

/cfg/domain #/adv

The **Advanced** menu appears.

The **Advanced** menu includes the following options:

Table 12
Configuring advanced settings

/cfg/domain #/adv

followed by:	
interface <interface ID>	References a previously created interface to serve as a backend interface for the domain. • **interface ID** is an integer that indicates the interface number. The default is 0. To configure the interface, use the **/cfg/sys/host #/interface** command (see "Configuring host interfaces" (page 268)).
log	Specifies the type of requests and operations to log. You are prompted to enter a comma-separated list of log types. Valid options are: • **all**—logs all options • **login**—logs portal logins and logouts • **http**—logs HTTP requests made from the portal • **portal**—logs non-HTTP portal operations, such as FTP and SMB file server access • **reject**—logs rejected requests The default is **login**. Each type of log generates its own set of syslog messages. The syslog messages include date, time, type of request, user, source IP address, and requested destination.

Configuring RADIUS accounting

The Nortel SNAS can be configured to provide support for logging administrative operations and user session start and stop messages to a RADIUS accounting server.

With RADIUS accounting enabled, the Nortel SNAS sends an accounting request start packet to the accounting server for each user who successfully authenticates to the Nortel SNAS domain. The start packet contains the following information:

- client user name
- Nortel SNAS device Real IP address (RIP)
- session ID

When the user session terminates, the Nortel SNAS sends an accounting request stop packet to the accounting server. The stop packet contains the following information:

- session ID
- session time
- cause of termination

Configure the RADIUS server in accordance with the recommendations in RFC 2866.

Certain Nortel SNAS -specific attributes are sent to the RADIUS server when you enable accounting (see “Configuring Nortel SNAS -specific attributes” (page 114)). In conjunction with custom plugins on RADIUS, these attributes can be used for more detailed monitoring of Nortel SNAS activity.

When you add an external RADIUS accounting server to the configuration, the server is automatically assigned an index number. Nortel SNAS accounting will be performed by an available server with the lowest index number. You can control accounting server usage by reassigning index numbers (see “Managing RADIUS accounting servers” (page 112)).

To configure the Nortel SNAS to support RADIUS accounting, use the following command:

```
/cfg/domain #/aaa/radacct
```

The **Radius Accounting** menu appears.

The **Radius Accounting** menu includes the following options:

Table 13
Configuring RADIUS accounting

`/cfg/domain #/aaa/radacct` **followed by:**	
`servers`	Accesses the **Radius Accounting Servers** menu, in order to configure external RADIUS accounting servers for the domain (see “Managing RADIUS accounting servers” (page 112)).
`domainattr`	Accesses the **Domain Attribute** menu, in order to configure Nortel SNAS -specific attributes to be sent to the accounting server (see “Configuring Nortel SNAS -specific attributes” (page 114)).

Table 13
Configuring RADIUS accounting (cont'd.)

/cfg/domain #/aaa/radacct **followed by:**	
ena	Enables RADIUS accounting. The default is disabled.
dis	Disables RADIUS accounting. The default is disabled.

Managing RADIUS accounting servers

To configure the Nortel SNAS to use external RADIUS accounting servers, use the following command:

/cfg/domain #/aaa/radacct/servers

The **Radius Accounting Servers** menu appears.

The **Radius Accounting Servers** menu includes the following options:

Table 14
Managing RADIUS accounting servers

/cfg/domain #/aaa/radacct/servers **followed by:**	
list	Lists the IP addresses of currently configured RADIUS accounting servers, by index number.
del <index number>	Removes the specified RADIUS accounting server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured RADIUS accounting servers, use the **list** command.

Table 14
Managing RADIUS accounting servers (cont'd.)

/cfg/domain #/aaa/radacct/servers **followed by:**	
add <IPaddr> <port> <shared secret>	Adds a RADIUS accounting server to the configuration. You are prompted to enter the following information: • **IPaddr**—the IP address of the accounting server • **port**—the TCP port number used for RADIUS accounting. The default is 1813. • **shared secret**—the password used to authenticate the Nortel SNAS to the accounting server Shared secret must be same in NSNA and RADIUS server. The system automatically assigns the next available index number to the server.
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of RADIUS accounting servers in the configuration. • index number—the index number you want the server to have • **IPaddr**—the IP address of the accounting server you are adding The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of RADIUS accounting servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

Configuring Nortel SNAS -specific attributes

The RADIUS accounting server uses Vendor-Id and Vendor-Type attributes in combination to identify the source of the accounting information. The attributes are sent to the RADIUS accounting server together with the accounting information for the logged in user.

You can assign vendor-specific codes to the Vendor-Id and Vendor-Type attributes for the Nortel SNAS domain. In this way, the RADIUS accounting server can provide separate accounting information for each Nortel SNAS domain.

Each vendor has a specific dictionary. The Vendor-Id specified for an attribute identifies the dictionary the RADIUS server will use to retrieve the attribute value. The Vendor-Type indicates the index number of the required entry in the dictionary file.

The Internet Assigned Numbers Authority (IANA) has designated SMI Network Management Private Enterprise Codes that can be assigned to the Vendor-Id attribute (see http://www.iana.org/assignments/enterprise-numbers).

RFC 2866 describes usage of the Vendor-Type attribute.

Contact your RADIUS system administrator for information about the vendor-specific attributes used by the external RADIUS accounting server.

To simplify the task of finding accounting entries in the RADIUS server log, do the following:

Step	Action
1	In the RADIUS server dictionary, define a descriptive string (for example, `NSNAS-Portal-ID`).
2	Map this string to the Vendor-Type value.
	--End--

To configure vendor-specific attributes in order to identify the Nortel SNAS domain, use the following command:

```
/cfg/domain #/aaa/radacct/domainattr
```

The **Domain Attribute** menu appears.

The **Domain Attribute** menu includes the following options:

Table 15
Configuring Nortel SNAS-specific attributes

/cfg/domain #/aaa/radacct/domainattr **followed by:**	
vendorid	Corresponds to the vendor-specific attribute used by the RADIUS accounting server to identify accounting information from the Nortel SNAS domain. The default Vendor-Id is 1872 (Alteon).
vendortype	Corresponds to the Vendor-Type value used in combination with the Vendor-Id to identify accounting information from the Nortel SNAS domain. The default Vendor-Type value is 3.

Configuring local DHCP services

The Nortel SNAS can be configured for DHCP services, to provide:

- support for non-NSNA network access devices including Nortel Ethernet Switch Models 325 / 425 / 450 / 470 and 2500 series and Ethernet Routing Switch models - 4500 series, 5500 series, 8300 and 8600 as well as third party switches, and support for multiple devices on a port (for example, when a hub is connected to the port).
  DHCP subnet type: **hub**.
- DNS server redirect from Nortel SNAS to the corporate DNS server, to optimize Nortel SNAS performance when **Filters only** enforcement is used. For more information on **Filters only** enforcement, see "Nortel SNAS enforcement types" (page 28).
  DHCP subnet type: **filter**
- a standard DHCP server that supports RFC 2131 in the context of the Nortel SNAS network architecture; that is, server to server unicast messages for DHCP relayed messages. For information on the Nortel SNAS network architecture, see *Nortel Secure Network Access Solution Guide, NN47230-200*, (formerly 320817).
  DHCP subnet type: **standard**

To configure DHCP services, use the following command:

/cfg/doamin #/dhcp

The DHCP menu appears.

The DHCP menu includes the following options:

Table 16
Configuring local DHCP services

/cfg/doamin #/dhcp **followed by:**	
subnet <number> <type> <name> <address> <netmask>	Initiates a series of prompts that define the DHCP subnet. • **number** is a unique number between 1 and 256 that you provide that the system uses to identify the subnet. The prompt is—**Enter DHCP subnet number (1-256):** • **type** is a Nortel SNAS term that defines the type of DHCP service. The prompt is—**Select one of hub, filter and standard:** See above the table for the application of each type. — **hub**: for support of network access devices that do not support SSCP, and multiple devices on a single port. — **filter**: to provide a mechanism for redirecting the client to the corporate DNS server when the network access points are NSNA network access points and **Filters only** enforcement is configured. — **standard**: for standard DHCP services that conform to RFC 2131 for DHCP relayed messages. Each type has a set of configuration options associated with it. For information on these options, see "Standard DHCP subnet type" (page 121), "Filter DHCP subnet type" (page 120), or "Hub DHCP subnet type" (page 118). • **name** refers to a name you provide for the subnet. The prompt is—**Set the subnet name:** • **address** is the subnet address. The prompt is—**Enter subnet network address:** • **netmask** is the subnet mask. The prompt is—**Enter subnet network mask:**
stdopts	Prompts you to identify and configure values for the standard DHCP options. As a minimum, you must configure Option 3 (Default Router), Option 6 (Domain Name Server), Option 15 (Domain Name), and Option 51 (Lease Time). When configuring Option 51 (Lease Time), the lease interval is specified in seconds. The values set at this level of the DHCP menus are applied globally to all DHCP subnets and types. You are provided with the option of changing the global values when specific DHCP settings are configured. See "DHCP Settings menu" (page 117).

Table 16
Configuring local DHCP services (cont'd.)

/cfg/doamin #/dhcp **followed by:**	
vendopts <number> <name> <value> <del>	Initiates a series of prompts that allow you to specify RFC 2132 vendor options. • **number** is a unique number between 1 and 254 that you provide that the system uses to identify the vendor options. The prompt is—**Enter vendor options number (1-254):** • **name** refers to a name you provide for this set of vendor options. The prompt is—**Set the vendor option name:** • **type** can be **ip**, **ip_list**, **u8**, **u16**, **u32**, **string**, or **bool**. • **value** refers to allowed values for the **type**, as per RFC2132. • **del** deletes the vendor options. The values set at this level of the DHCP menus are applied globally to all DHCP subnets and types. You are provided with the option of changing the global values when specific DHCP settings are configured. See "DHCP Settings menu" (page 117).
quick	Provides a quick DHCP setup wizard. Options are described under the DHCP type: "Standard DHCP subnet type" (page 121), "Filter DHCP subnet type" (page 120), or "Hub DHCP subnet type" (page 118).

DHCP Settings menu

The DHCP settings menu whenever you select an option that requires a range of IP addresses. This occurs when configuring:

- the **settings** for the standard DHCP subnet type
- the **known** and **unknown** ranges for the filter DHCP subnet type
- the **red**, **yellow**, and **green** ranges for the hub DHCP subnet type.

The DHCP settings menu includes the following options:

Table 17
DHCP Settings menu

ranges <list> <del> <add> <insert> <move>	Establishes the lower and upper IP addresses of a range of IP addresses. More than one range can be configured. • **list** a list of current ranges. The format of the output is `#: IP address : IP address` where # is an integer that specifies the index of the range. The index is required to delete, insert, or move a range. • **del #** deletes the range with index number **#.** • **add IPaddressLower IPaddressUpper** adds a new range with lower and upper limits defined by **IPaddressLower** and **IPaddressUpper**, respectively.

	• **insert # IPaddressLower IPaddressUpper** inserts a new range above the range having index number **#**. For example, if **#** is 3, the new range is assigned index number 3 and the current range with index number 3 is reassigned to index number 4. The lower and upper limits of the new range are defined by **IPaddressLower** and **IPaddressUpper**, respectively. • **move #A #B** changes the index number of range **#A** to **#B** and changes the index number of **#B** to **#A**. That is, the ranges switch places in the range list.
stdopts	Prompts you to identify and configure values for the standard DHCP options. If you have configured the DHCP standard options using the **stdopts** command from the **/cfg/doamin #/dhcp** menu, those values carry through to here. If you change the values here, the new values only apply to the range(s) you are defining here.
vendopts <number> <name> <value> <del>	Initiates a series of prompts that allow you to specify RFC 2132 vendor options. If you have configured the vendor options using the **vendopts** command from the **/cfg/doamin #/dhcp** menu, those values carry through to here. If you change the values here, the new values only apply to the range(s) you are defining here. • **number** is a unique number between 1 and 254 that you provide that the system uses to identify the vendor options. The prompt is—**Enter vendor options number (1-254):** • **name** refers to a name you provide for this set of vendor options. The prompt is—**Set the vendor option name:** • **type** can be **ip**, **ip_list**, **u8**, **u16**, **u32**, **string**, or **bool**. • **value** refers to allowed values for the **type**, as per RFC2132. • **del** deletes the vendor options.

Hub DHCP subnet type

The hub DHCP subnet type is used to support non-NSNA network access devices, and multiple devices on a single port (for example, hubs). This section assumes you are familiar with the information in "Configuring local DHCP services" (page 115).

The end-to-end configuration process includes:

- creating a VLAN that includes all ports on network access point ports that are participating in the NSNA configuration
- configuring three IP address ranges within the VLAN on the Nortel SNAS; these define the red, yellow, and green enforcement zones
- establishing filters for the red range on the network access points that:

— direct all DNS requests to the Nortel SNAS

— allow HTTP, HTTPS, ICMP, and DHCP traffic to access the Nortel SNAS subnet only

- creating access control lists or filters on upstream routers for the yellow and green address ranges, to direct connection requests to appropriate network resources
- configuring the router that serves the Nortel SNAS to relay DHCP requests to the Nortel SNAS management IP address (MIP); RFC 2131 server to server unicast messages are supported
- configuring the VoIP VLAN (see "Nortel SNAS enforcement types" (page 28))
- configuring Nortel SNAS groups to meet your authentication requirements (see "Configuring groups" (page 156)for more information).

The menu for the hub DHCP subnet type includes:

Table 18
Hub DHCP subnet type

type	the current DHCP subnet type and prompts you to change or reenter the type. Enter: **hub**.
name	the current name of the subnet and prompts you to change or reenter the name. Enter a name.
address	the current network address of the subnet and prompts you to change or reenter the address.
netmask	the current network mask of the subnet and prompts you to change or reenter the network mask.
phone	Specify a phone signature for each type of IP phone connected to the network. Supported phone types and their signatures are: • Nortel i2001 — Nortel-i200 • Nortel i2002 — Nortel-i200 • Nortel i2004 — Nortel-i200 • Nortel i2007 — Nortel-i200
relaygreen	When the Nortel SNAS reassigns clients to a green enforcement zone, they can be directed to the green zone managed by the Nortel SNAS or they can be directed to an external DHCP server, generally your corporate server. To direct the clients to an external DHCP server, enter the IP address of the server here and do not configure the **green** zone.
vlan	Enter a name for the VLAN.

Table 18
Hub DHCP subnet type (cont'd.)

red	Configures the IP address range and options for the red enforcement zone. See "DHCP Settings menu" (page 117). Enter the IP address range for the red enforcement zone. Enter the pVIP of the Nortel SNAS for the DNS address (option 6). It is recommended that you configure a short lease time (option 51).
yellow	Defines the yellow enforcement zone. See "DHCP Settings menu" (page 117). Enter the IP address range for the yellow enforcement zone. Enter the IP address of your corporate remediation server for the DNS address (option 6).
green	Defines the green enforcement zone. See "DHCP Settings menu" (page 117). Enter the IP address range for the green enforcement zone. Enter the IP address of your corporate DHCP server for the DNS address (option 6).
ena	Enables the subnet.
dis	Disables the subnet.
del	Deletes the subnet.

Filter DHCP subnet type

The filter DHCP subnet type provides a mechanism for redirecting the client to the corporate DNS server when the network access points are NSNA network access devices and **Filter only** enforcement is used. This section assumes you are familiar with the information in "Configuring local DHCP services" (page 115).

Background: When the Nortel SNAS determines that a client can be moved from the Red enforcement zone, it directs Nortel Health Agent to initiate an ipconfig release/renew to change the IP address of the client. There are a number of situations where this Nortel Health Agent action does not occur (for information, see "Configuring groups" (page 156)). In these situations, the IP address of the client remains as initially obtained from the DHCP server and the DNS server for the client continues to be the Nortel SNAS. The result is that all DNS resolution is handled by the Nortel SNAS. The filter DHCP subnet type allows you to optomize network performance by redirecting DNS services from the Nortel SNAS to the corporate DNS server.

The menu for the filter DHCP subnet type includes:

Table 19
Filter DHCP subnet type

type	the current DHCP subnet type and prompts you to change or reenter the type. Enter: **filter**.
name	the current name of the subnet and prompts you to change or reenter the name. Enter a name.
address	the current network address of the subnet and prompts you to change or reenter the address. Enter an address consistent with your network environment.
netmask	the current network mask of the subnet and prompts you to change or reenter the network mask. Enter a network mask consistent with your network environment.
known	See "DHCP Settings menu" (page 117). The status of the client is changed from "unknown" to "known" after authentication, and successful integrity checking when applicable. Configure **stdopts** to point to the network domain name server.
unknown	See "DHCP Settings menu" (page 117). The client is automatically assigned "unknown" status when the connection is initiated. This is the Red enforcement zone for the filter DHCP subnet type. No configuration is required.
ena	Enables the subnet.
dis	Disables the subnet.
del	Deletes the subnet.

Standard DHCP subnet type

The standard DHCP subnet type provides DHCP services that conform to RFC 2131 for server to server unicast messages. This section assumes you are familiar with the information in "Configuring local DHCP services" (page 115).

The menu for the standard DHCP subnet type includes:

Table 20
Standard DHCP subnet type

type	the current DHCP subnet type and prompts you to change or reenter the type.
name	the current name of the subnet and prompts you to change or reenter the name.

Table 20
Standard DHCP subnet type (cont'd.)

address	the current network address of the subnet and prompts you to change or reenter the address.
netmask	the current network mask of the subnet and prompts you to change or reenter the network mask.
settings	See "DHCP Settings menu" (page 117).
ena	Enables the subnet.
dis	Disables the subnet.
del	Deletes the subnet.

Managing local DHCP leases

The following commands are provided for managing DHCP leases:

Table 21
Managing local DHCP leases

/info/dhcp/ list <list> <del> <stats>	Use **list** to list current DHCP leases. See below. Use **del** to delete current DHCP leases. See below. Use **stats** to display information on all leases. The tabulated display has these columns: Dom (domain); Snet (Subnet number); Type (**S**tandard, **F**ilter, **H**ub); Network (subnet address); Total (total number of leases); and the total number of leases in each zone (Red, Green, Yellow, Unknown, Known).
/info/dhcp/ list/ <addr> <subnet> <all>	Use **addr** together with an IP address or a MAC address to list the DHCP lease for the address. Use **subnet** together with a subnet address and mask to list DHCP leases for the subnet. Use **all** to list all DHCP leases.
/info/dhcp/ del/ <addr> <subnet> <all>	Use **addr** together with an IP address or a MAC address to delete the DHCP lease for the address. Use **subnet** together with a subnet address and mask to delete DHCP leases for the subnet. Use **all** to delete all DHCP leases.

Creation of the location

To create the location, use the following command:

/cfg/domain #/location

Enter the location number. Creates the location #.
Enter the name of the location.

The **Location** menu appears.

The **Location** menu includes the following options:

/cfg/domain #/location **followed by:**	
name	A string that specifies a unique location name.
locations <add> <del> <list>	Manage switch ip, unit/port details. • **add**—adds switch, unit/portr. • **del**—deletes switch, unit/port. • **list**—lists switch, unit/port.
del	Removes location from the configuration.

Creation of the locations

To create the locations, use the following command:

/cfg/domain/location/locations

The **Location List** menu appears.

The **Location List** menu includes the following options:

/cfg/domain/location/locations **followed by:**	
add <switch Ip> <unit/port>	Adds locations. • **switch Ip**—specify the Switch Ip. • **unit/port**—specify the Unit/Port.

/cfg/domain/location/locations **followed by:**	
del <index number>	Removes the locations from the configuration. • **index number**—specify the index number. • **unit/port**—specify the Unit/Port.
list	lists all the configured locations.

Configuring Lumension PatchLink integration

Nortel SNAS is integrated with the Lumension PatchLink security patch management system, which allows to proactively enforce user and device compliance by ensuring that devices are properly patched and up-to-date.

PatchLink server is a patch and vulnerability management solution. It works in an Agent mode, where an installed agent (system service) communicates to a central PatchLink server and updates the system as and when patches are available. Patchlink solution is integrated to verify the compliance status of the client with Nortel SNAS.

To create the patchlink server, use the following command:

/cfg/domain/patchlink

The **PatchLink Servers** menu appears.

The **PatchLink Servers** menu includes the following options:

/cfg/domain/patchlink **followed by:**	
add <IP address> <username> <password>	Adds a patch link server. • **IP address**—specify the IP address. • **username**—string that specifies a unique user login name. • **password**—the password that applies to the user you specified.

/cfg/domain/patchlink **followed by:**	
del <index number>	Deletes the patch link server from the patch link list. • **index number**—is the identification number automatically assigned to the patch link server, when you added the patch link server to the configuration.
list	Lists all patch link server added by user name, password.
ena	Enables the patch link server.
dis	Disables the patch link server.

Configuration of the RADIUS server

This chapter includes the following topics:

Overview of RADIUS server

The Nortel SNAS is integrated with full featured RADIUS server. The RADIUS server is used to authenticate users through PAP or CHAP authentication methods. It also works in a more complex 802.1x environment, which supports EAP-MD5, TLS, PEAP, and TTLS authentication methods.

Radius server configuration includes the RADIUS realms, clients, authentication methods, EAP authentication methods, dictionary, accounting logs, and accounting ports components.

802.1x functionality

Integration of RADIUS server with the Nortel Health Agent’s 802.1x supports 802.1x for user authentication and health assessment in the Nortel SNAS.

Roadmap of RADIUS server configuration commands

The following roadmap lists the Command Line Interface (CLI) commands to configure Remote Authentication Dial-In User service (RADIUS). Use this list as a quick reference.

Command	Parameter
/cfg/domain/radius	authentication port
	accounting port
/cfg/domain/radius/clients	list
	del <index number>
	add <client IP address> <shared secret >
	insert <index number> <client IP address> <shared secret>
	move <index number> <destination index number>
/cfg/domain/radius/realms	list
	del <index number>
	add <realm name / ip address> <authentication server id>>
	insert <index number> <realm name / ip address> <authentication server id>
	move <index number> <destination index number>
/cfg/domain/radius/dictionary	default
	import <protocol> <host> <filename>
	export <protocol> <host> <filename> <venderid>
	view
	del <vendor id>
	clear
	list
/cfg/domain/radius/accounting	view
	export <protocol> <host> <filename>
	clear
/cfg/domain/radius/methods	list
	del <index number>
	add <method name>

Command	Parameter
	insert <index number> <method name>
	move <index number> <destination index number>
/cfg/domain/radius/eapmethods	**list**
	del <index number>
	add <method type> <module name>
	insert <index number> <method type> <module name>
	move <index number> <destination index number>
/cfg/domain/radius/cert	**current value**
	select the certificate
/cfg/domain/radius/cacert	**current value**
	select the certificate

Configuration of the RADIUS server

To configure the RADIUS server, use the following command

/cfg/domain/radius

The **RADIUS Server** menu appears.

The **RADIUS Server** menu includes the following options:

/cfg/domain/radius **followed by:**	
authentication port	Specify the authentication port. Default value is 1812.
accounting port	Specify the accounting port. Default value is 1813.

Configuration of the client

To configure the client, use the following command:

/cfg/domain/radius/clients

The **RADIUS Clients** menu appears.

The **RADIUS Clients** menu includes the following options:

/cfg/domain/radius/clients **followed by:**	
list	Lists the IP addresses of currently configured clients, by index number.
del <index number>	Removes the specified client from the current configuration. The index numbers of the remaining entries adjust accordingly. • **index number**—specify the index number. To view the index numbers of all configured clients use the list command.
add <client IP address> <shared secret>	Adds a client to the configuration list. • **client IP address**—the IP address of the client. • **shared secret**—the password used to authenticate the Nortel SNAS to the RADIUS clients.

/cfg/domain/radius/clients **followed by:**	
insert <index number> <client IP address> <shared secret>	Inserts a client at a particular position in the list of clients in the configuration. • **index number**—specify the index number. • **client IP address** —specify the IP address of the client. • **shared secret**—the password used to authenticate the Nortel SNAS to the clients.
move <index number> <destination index>	Moves a client up or down the list of clients in the configuration. • **index number**—the original index number of the client you want to move • **destination index**—the index number representing the new position of the server in the list.

Configuration of the realms

To configure the realms, use the following command:

/cfg/domain/radius/realm

The **RADIUS Realms** menu appears.

The **RADIUS Realms** menu includes the following options:

/cfg/domain/radius/realms **followed by:**	
list	Lists the IP addresses of currently configured realms, by index number.

/cfg/domain/radius/realms **followed by:**	
del <index number>	Removes the specified realms from the current configuration. The index numbers of the remaining entries adjust accordingly. • **index number**—the original index number of the client you want to remove. To view the index numbers of all configured clients use the list command.
add <realm name> <authentication server id>	Adds a realm to the configuration. • **realm name**—is a string identifying the realm names. • **authentication server id**—select the authentication server id. It the list based on the authentication servers configured on the device.
insert <index number> <realm name> <authentication server id>	Inserts a realm at a particular position in the list of clients in the configuration. • **index number**—the index number you want the realms to have. • **realm name**—is a string identifying the realm names. • **authentication server id**—select the authentication server id. It the list based on the authentication servers configured on the device.
move <index number> <destination index number>	Moves a client up or down the list of Realms in the configuration. • **index number**—the original index number of the realms you want to move. • **destination index**—the index number representing the new position of the realms in the list.

Configuration of the dictionary

To configure the dictionary, use the following command:

/cfg/domain/radius/dictionary

The **RADIUS Attribute Dictionary** menu appears.

The **RADIUS Attribute Dictionary** menu includes the following options:

/cfg/domain/radius/dictionary **followed by:**	
default	Sets default RADIUS attribute configuration.
import <protocol> <server> <filename>	Imports dictionary from TFTP/FTP/SCP/SFTP server. • **protocol**—protocol is the import protocol. Options are tftp|ftp|scp|sftp. Default value is tftp. • **server**—specify the hostname or IP address of the server. • **filename**—specify the name of the database file on the server.
export <protocol> <server> <filename> <vender id>	Exports dictionary to TFTP/FTP/SCP/SFTP server. • **protocol**—protocol is the export protocol. Options are tftp|ftp|scp|sftp. Default value is tftp. • **server**—specify the hostname or IP address of the server. • **filename**—is a name of the database file on the server. • **vender id**—corresponds to the vendor-specific attribute used by the RADIUS server.
view	Views the vendor dictionary.
delete <index number>	Removes the specified vendor dictionary. • **index number**—is the identification number automatically assigned to the dictionary when you added the dictionary to the configuration.specify the index number to remove.

/cfg/domain/radius/dictionary **followed by:**	
clear	Clears all the vendor dictionary.
list	Lists configured vendor dictionaries by index number.

Configuration of the RADIUS accounting

To configure the RADIUS accounting, use the following command:

/cfg/domain/radius/accounting

The **RADIUS Accounting** menu appears.

The **RADIUS Accounting** menu includes the following options:

/cfg/domain/radius/accounting **followed by:**	
view	Shows the accounting log information for the following: • Time • User-name • Status-Type • Terminate-cause
export <protocol> <hostname or IP address> <filename>	Exports the accounting log to FTP/FTP/SCP/SFTP server • **protocol**—is the export protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **hostname or IP address**—is the hostname or IP address of the server. • **filename**—specify the filename on the server.
clear	Clears the accounting log information.

Configuration of the RADIUS authentication methods

To configure the RADIUS authentication methods, use the following command:

/cfg/domain/radius/methods

The **RADIUS Authentication Methods** menu appears.

The **RADIUS Authentication Methods** menu includes the following options:

/cfg/domain/radius/methods **followed by:**	
list	Lists the authentication methods: 1. mac 2. proxy 3. acct 4. pap 5. chap 6. mschapv1 7. mschapv2 8. eap
del <index number>	Removes the specified methods from the current configuration.The index numbers of the remaining entries adjust accordingly. • **index number**—is the identification number automatically assigned to the method,when you added the method to the configuration. specify the index number to remove from the configuration
add <method name>	Adds a method to the configuration. • **method name**—is a string that must be unique in the domain. The maximum allowable length of the string is 255 characters, but Nortel recommends a maximum of 32 characters.

/cfg/domain/radius/methods **followed by:**	
insert <index number> <method name>	Inserts a methods at a particular position in the list • **index number**—is the identification number automatically assigned to the method,when you added the method to the configuration.specify the index number. • **method name**—is a string that must be unique. The maximum allowable length of the string is 255 characters, but Nortel recommends a maximum of 32 characters.
move <index number> <destination index>	Moves a method up or down the list . • **index number**—the original index number of the method you want to move. • **destination index** —the index number representing the new position of the method in the list.

Configuration of the EAP authentication methods

To configure the EAP authentication methods, use the following command:

/cfg/domain/radius/eapmethods

The **EAP Authentication Methods** menu appears.

The **EAP Authentication Methods** menu includes the following options:

/cfg/domain/radius/eapmethods **followed by:**	
list	Lists the EAP authentication methods. • 1: 4 : eap_md5 • 2 :6 : eap_gtc • 3: 26 : eap_mschapv2 • 4: 13 : eap_tls • 5: 21 : eap_tls • 6 :25 :eap_tls

/cfg/domain/radius/eapmethods **followed by:**	
del <index number>	Removes the specified EAP method from the current configuration. The index numbers of the remaining entries adjust accordingly. • **index number**—is the identification number automatically assigned to the EAP method, when you added the EAPmethod to the configuration.
add <method type> <module name>	Adds a EAP method to the configuration. • **method type**—Specify the method type. • **module name**—is a string that must be unique. The maximum allowable length of the string is 255 characters, but Nortel recommends a maximum of 32 characters. Specify the module name.
insert <index number> <method type> <module name>	Inserts a EAP method at a particular position in the list. • **index number**—is the identification number automatically assigned to the EAP method,when you added the method to the configuration. Specify the index number. • **method type**—Specify the method type. • **method name**—is a string that must be unique in the domain. The maximum allowable length of the string is 255 characters, but Nortel recommends a maximum of 32 characters. Specify the module name.
move <index number> <destination index>	Moves a EAP Method up or down the list . • **index number**—the original index number of the EAP Methods. • **destination index**—the index number representing the new position of the EAP method in the lists.

Select the server certificate

Select the server certificate from the list, use the following command:

/cfg/domain/radius/cert

This includes the following options:

/cfg/domain/radius/cert **followed by:**	
current value	The current server certificate number appears.
select the certificate	Specify the server certificate number. The value ranges from 1 to 1500. The certificate number refers to certificates stored in the certificate repository.

Select the CA certificate

Select the server certificate from the list, use the following command:

/cfg/domain x/radius/cacert

This includes the following options:

/cfg/domain/radius/cacert **followed by:**	
current value	The current CA certificate number appears.
select the CA certificate	Specify the CA certificate number. The value ranges from 1 to 1500. The CA certificate number refers to certificates stored in the certificate repository.

Configuration of Microsoft NAP Interoperability

This chapter includes the following topics:

Roadmap of NAP configuration commands

The following roadmap lists the Command Line Interface (CLI) commands to configure Network Access Protection (NAP). Use this list as a quick reference.

Command	Parameter
`/cfg/domain/nap`	`autorem`
`/cfg/domain/nap/probation`	`ena [<true|false>]`
	`dis [<true|false>]`
	`date <date>`
	`time <time>`
`/cfg/domain/nap/moreinfo`	`troubleshooting URL`
`/cfg/domain/nap`	`pdp <local|remote>`
`/cfg/domain/nap/servers`	`list <ip> <port> <secret>`
	`del`
	`add <server IP address> <server port> <shared secret>`

Command	Parameter
	insert <position> <ip> <port> <secret>
	move <index number> <destination index number>
/cfg/domain/nap/shvs	**list**
	del
	add <vendor ID> <component ID> <module name>
	insert <position> <vendor ID> <component ID> <module name>
	move <index number> <destination index number>
/cfg/domain/nap/wshv	**firewall** on|off
	autoupdate on|off
	virus enabled true|false uptodate true|false
	spyware enabled true|false uptodate true|false
	secupdates <enabled> <severity> <lastsync> <wsus> <winupdate>

Configuration of NAP Interoperability

Microsoft Network Access Protection (NAP), introduced with Windows Vista and Windows Server is a new set of operating system components that provides a platform for protected access to private networks. The NAP platform provides an integrated way of detecting the health state of a network client, which attempts to connect to a network and restricts the access of the network client until the policy requirements for connecting to the network are met. The NSNA NAP interoperability architecture allows you to deploy both the NSNA solution and the Network Access Protection (NAP) in a symbiotic manner. It also allows you to enforce security policies for network access using NSNA and NAP together, leveraging the strengths of both products. It also deploys the NAP clients with or without a Microsoft NPS server present on your network. If the Microsoft NPS server is available, it is consulted and its response are used in a configurable way to enhance the access decision made by the Nortel SNAS. If your system does not contain a Microsoft NPS server in place, it can still deploy clients with NAP support enabled and then adds a Microsoft NPS server if desired.

Windows 802.1x Supplicant—The Nortel Health Agent integrated with the Microsoft NAP Agent provides a robust EAP supplicant for Windows Vista and XP Operating Systems.

To configure the Network Access Protection (NAP), use the following command:

cfg/domain/nap

The **NAP** menu appears.

The **NAP** menu includes the following options:

cfg/domain/nap/ followed by:	
autorem	Sets necessary updates to allow a noncompliant computer to become compliant. Values: false and true. default: false.
probation	Probation Settings
moreinfo<Troublshooting URL>	Set Troublshooting URL
pdp	Select the policy decision point. Values: local and remote. default: local
servers	Remote Network Policy Servers
shvs	System Health Validators
wshv	Windows System Health Validator

Probation Settings

To configure the probation settingsg, use the following command:

cfg/domain/nap/probation

The **Probation Settings** menu includes the following options:

cfg/domain/nap/probation **followed by:**	
ena	Enables full access for a limited time.
dis	Disables full access for a limited time.
date	Sets the date (YYYY-MM-DD)
time	Sets the time (24-hour, HH:MM:SS)

Remote Network Policy Servers

To create the remote network policy servers, use the following command:

cfg/domain/nap/servers

The **Remote Network Policy Servers** menu includes the following options:

cfg/domain/nap/servers **followed by:**	
list	Lists the IP addresses of currently configured remote network policy servers, by index number..
del <index number>	Removes the specified remote network policy server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured remote network policy servers, use the **list** command.
add <IP address> <port> <shared secret>	Adds a server to the configuration. • **IP address**—specify the IP address of the server • **port**—the TCP port number. • **shared secret**—specify the password.
insert <index number> <IPaddr> <port> <shared secret>	Inserts a server at a particular position in the list of remote network policy server in the configuration. • **index number** —the index number you want the server to have • **IPaddr**—specify the IP address of the remote network policy serverr you are adding • **port**—specify the TCP port number. • **shared secret**—specify the password.

cfg/domain/nap/servers **followed by:**	
	The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of remote network policy server in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

System Health Validators

To create the system health validators, use the following command:

cfg/domain/nap/shvs

The **System Health Validators** menu includes the following options:

cfg/domain/nap/shvs **followed by:**	
list <vendor ID> <component ID> <module name>	Lists the vendor ID, component ID and module name.
del <index number>	Removes the specified system health validators from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured remote network policy servers, use the **list** command.
add <vendor ID> <component ID> <module name>	Adds a system health validators to the configuration. • **vendor ID**—specify the vender ID. • **component ID**—specify the component ID. • **module name**—specify the module name.

cfg/domain/nap/shvs followed by:	
insert <index number> <vendor ID> <component ID> <module name>	Inserts a system health validators at a particular position in the configuration. • **index number** —the index number you want the system health validators to have • **vendor ID**—specify the vendor ID you are adding • **component ID**—specify the component ID.. • **module name**—specify the module name. The index number you specify must be in use. The index numbers of existing system health validators with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a system health validators up or down the list of System Health Validators in the configuration. • **index number**—the original index number of the system health validators you want to move • **new index number**—the index number representing the new position of the system health validators in the list The index numbers of the remaining entries adjust accordingly.

Configuration of Windows System Health Validator

To create the windows system health validator, use the following command:

cfg/domain/nap/wshv

The **Windows System Health Validators** menu includes the following options:

cfg/domain/nap/wshv followed by:	
firewall	Enables or disables the firewall application. Values: on and off default: on

cfg/domain/nap/wshv **followed by:**	
virus <antivirus> <uptodate>	Virus Protection. • **antivirus**—Enables or disables the antivirus. Values: true and false default: false • **uptodate**—Specifies whether the antivirus is up to date or not. Values: true and false default: true.
spyware <antispy> <uptodate>	Spyware Protection. • **antispy** —Enables or disables the antispyware. Values: true and false default: false • **uptodate**—Specifies whether the antispyware is up to date or not. Values: true and false default: true
secupdates<enabled> <severity> <lastsync> <wsus> <winupdate>	Security Updates Protection. • **enabled**—enables or disables the Windows System Health Verifier (WSHV) to validate the Windows endpoint's current software security patch levels. Microsoft Windows security update patches are Windows update patches that fix specific software security vulnerabilities. Values: true and false default: false • **severity**—security Updates Severity instructs the Windows System Health Verifier (WSHV) to validate the minimum level of all Windows security update patches on the Windows endpoint. For instance, if the Security Updates Severity is set to "critical" the Windows endpoint must have all Microsoft Windows security update patches designated by the Microsoft Research Center as "critical" installed for the endpoint to be considered policy complaint. Values: critical, important, moderate, low, and all If the Security Updates Severity is set to "important" the Windows endpoint must have security update patches designated as "important" or higher installed to be considered policy complaint (so all updates designated as either "important" or "critical").

cfg/domain/nap/wshv **followed by:**	
	This setting is only applicable when Security Updates Protection is "true." default: important • **lastsync**—designates the duration of time allowed to pass since the Windows endpoint was last updated its own copy of its Windows security update list from its security update source (Windows Update or Windows Server Update Service). Only if the Windows endpoint has synchronized its security update information from its update source within this time is the endpoint considered policy compliant. This setting is only applicable when Security Updates Protection is "true." default: 86400 seconds (1 day) • **wsus**—designates whether Windows Server Update Service (WSUS) is an acceptable source for endpoints to obtain their Windows security update information. When the endpoint reports its security update status, it will do so with respect to the security updates it knows about (local copy) and the source where it obtained its security updates. Values: true and false If set to "true" the WSHV considers WSUS as an acceptable source for the endpoint and accepts the endpoint's security update status. This setting is only applicable when Security Updates Protection is "true." default: false • **winupdate**—designates whether Microsoft's Windows Update is an acceptable source for endpoints to obtain their Windows security update information. When the endpoint reports its security update status, it will do so with respect to the security updates it knows about (local copy) and the source where it obtained its security updates. Values: true and false If set to "true" the WSHV considers Windows Update as an acceptable source for the endpoint and accepts the endpoint's security update status. This setting is only applicable when Security Updates Protection is "true."

cfg/domain/nap/wshv **followed by:**	
	default: false
autoupdate	Enables or disables the automatic updates. Values: on and off default: on

Configuring groups and profiles

This chapter includes the following topics:

Overview

This section includes the following topics:

- “Groups” (page 150)
- “Linksets” (page 151)
- “SRS rule” (page 151)
- “Extended profiles” (page 151)

For more information about groups and extended profiles in the Nortel SNAS, see *Nortel Secure Network Access Solution Guide*, (NN47230-200).

Groups

The Nortel SNAS determines which VLANs users are authorized to access, based on group membership.

When a user logs on to the Nortel SNAS domain, the authentication method returns the group name associated with the user's credentials. The Nortel SNAS then maps the user to groups defined on the Nortel SNAS. You can define up to 1023 groups in the Nortel SNAS domain.

Each group's data include the following configurable parameters:

- linksets
- Nortel Health Agent SRS rule
- extended profiles

After the user has been authenticated, the Nortel SNAS checks the groups defined for the domain to match the group name returned from the authentication database. For the duration of the user's login session, the Nortel SNAS maintains a record of the group matched to the user.

When the Nortel SNAS has identified the matching group, it applies group data to the user as follows:

- linksets—All linksets configured for the group of which the user is a member display on the user's portal page (see "Linksets" (page 151)).
- Nortel Health Agent SRS rule—The Nortel Health Agent host integrity check uses the criteria specified in the SRS rule assigned to the group.
- extended profiles—The Nortel SNAS checks the group to identify if there is an applicable extended profile (see "Extended profiles" (page 151)).

For information about configuring a group, see "Configuring groups" (page 156).

Default group

You can configure a group to be the default group, with limited access rights. If the group name returned from the authentication database does not match any group defined on the Nortel SNAS, the Nortel SNAS will map the user to the default group.

To create a default group, see "Creating a default group" (page 169).

Linksets

A linkset is a set of links that display on the portal page, so that the user can easily access internal or external web sites, servers, or applications. After the user has been authenticated, the user's portal page all the linksets associated with the group to which the user belongs. The user's portal page also all the linksets associated with the user's extended profile.

When mapping linksets to groups or extended profiles, make sure that the access rules specified for the profile do not contradict the links defined for the linkset.

For information about creating and configuring the linksets, see "Configuring linksets" (page 251).

For information about mapping the linksets to groups, see "Mapping linksets to a group or profile" (page 167).

SRS rule

The SRS rule specified for the group is the set of operating system and other software criteria that constitute the host integrity check performed by the Nortel Health Agent applet. The SRS rule can be a composite of other rules, but there is only one SRS rule for the group. Each group can have a different SRS rule.

You cannot configure SRS rules using the CLI.

If you ran the quick setup wizard during the initial setup, you specified the action to result if the SRS rule check fails. You can rerun the wizard at any time by using the **`/cfg/doamin #/aaa/nha/quick`** command. If you want to change the SRS rule check result, use the **`/cfg/doamin #/aaa/nha/action`** command (see "Configuring the Nortel Health Agent check" (page 92)).

Extended profiles

Passing or failing the SRS rule check is the only authorization control provided at the group level. This is the base profile. In future releases of the Nortel SNAS software, extended profiles will provide a mechanism to achieve more granular authorization control, based on specific characteristics of the user's connection. You can define up to 63 extended profiles for each group.

In Nortel Secure Network Access Switch Software Release 1.6.1, the data for an extended profile include the following configurable parameters:

- linksets
- the VLAN which the user is authorized to access

Each extended profile references a client filter in a one-to-one relationship. With Nortel Secure Network Access Switch Software Release 1.6.1, you can configure the Nortel Health Agent check result as the criterion for the client filters, in order to establish the user's security status.

The client filter referenced in the extended profile determines whether the extended profile data will be applied to the user. After the user has been authenticated and the Nortel Health Agent host integrity check has been conducted, the Nortel SNAS checks the group's extended profiles in sequence, in order of the profile IDs, for a match between the client filter conditions and the user's security status. When it finds a match, the Nortel SNAS applies that particular extended profile's data to the user. Data defined for the base profile (for example, linksets) are appended to the extended profile's data. If the Nortel SNAS finds no match in any of the extended profiles, it applies the base profile data.

For information about configuring client filters, see "Configuring client filters" (page 162).

For information about configuring extended profiles, see "Configuring extended profiles" (page 164).

Before you begin

Before you configure groups, client filters, and extended profiles on the Nortel SNAS, complete the following tasks:

Step	Action
1	Create the linksets, if desired (see "Linksets and links" (page 234)).
2	Create the SRS rules (see *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*,), and for BBI (see *Nortel Secure Network Access Switch Configuration — Using the BBI* (NN47230-500)).
3	If authentication services have already been configured, ascertain the group names used by the authentication services. Group names defined on the Nortel SNAS must correspond to group names used by the authentication services. Table 22 "Group names in the Nortel SNAS and authentication services" (page 153) summarizes the requirements for the various authentication methods.

--End--

Table 22
Group names in the Nortel SNAS and authentication services

Authentication method	Group name on the Nortel SNAS must correspond to...
RADIUS	A group name defined in the vendor-specific attribute used by the RADIUS server. Contact your RADIUS system administrator for information.
LDAP	A group name defined in the LDAP group attribute used by the LDAP server. Contact your LDAP system administrator for information.
Local database	A group name used in the database. The group name is for internal use to control access to intranet resources according to the associated access rules. When you add a user to the local database, you map the user to one or more of the defined user groups.

Configuring groups and extended profiles

The basic steps to configure groups and extended profiles on the Nortel SNAS using the CLI are:

Step	Action
1	Configure the group (see “Configuring groups” (page 156)).
2	Configure the client filters that will be referenced in the extended profiles (see “Configuring client filters” (page 162)). The client filters can be referenced by all extended profiles in the domain.
3	Configure the extended profiles for the group (see “Configuring extended profiles” (page 164)).
4	Map the linksets to the group and extended profiles (see “Mapping linksets to a group or profile” (page 167)).
5	Create a default group, if desired (see “Creating a default group” (page 169)).
	--End--

Roadmap of group and profile commands

The following roadmap lists all the CLI commands to configure groups, client filters, extended profiles, and linkset mappings. Use this list as a quick reference or click on any entry for more information:

Table 23
Roadmap of CLI commands

Command	Parameter
/cfg/doamin #/aaa/group <group ID>	name <name>
	restrict
	srs <SRS rule name>
	agentmode <runonce | continuous | never>
	mactrust <bypass | none>
	enftype <filter_only | vlan_filter>
	macreg <true | false>
	reguser <true | false>
	admrights <user> <passwd> <action> <reset>
	comment <comment>
	del
/cfg/doamin #/aaa/filter <filter ID>	name <name>
	srs <true | false | ignore>
	comment <comment>
	del
/cfg/doamin #/aaa/group <group ID | group name>/extend [<profile ID>]	filter <name>
	vlan <name>
	linkset
	del
/cfg/doamin #/aaa/group #/linkset	list
	del <index number>
	add <linkset name>
	insert <index number> <linkset name>
	move <index number> <new index number>
/cfg/doamin #/aaa/group #/extend #/linkset	list
	del <index number>
	add <linkset name>

Table 23
Roadmap of CLI commands (cont'd.)

Command	Parameter
	`insert <index number> <linkset name>`
	`move <index number> <new index number>`
`cfg/domain #/aaa/group #/sessionttl`	`Usage: sessionttl <ttl>`
`cfg/domain #/aaa/group #/locations`	`Usage: cachepass <true|false>`
`/cfg/doamin #/aaa/group #/radattr/`	`list`
	`Usage: list <vendor> <id> <value>`
	`Usage: del <index>`
	`Usage: add`
	`Usage: add <vendor> <id> <value>`
	`Usage: insert <position> <vendor> <id> <>value`
	`Usage: move <value> <value>`
`cfg/domain #/aaa/group #/cachepass`	`Usage: cachepass <true|false>`
`cfg/domain #/aaa/group #/syscredent`	
`/cfg/doamin #/aaa/defgroup <group name>`	

Configuring groups

To create and configure a group, use the following command:

/cfg/doamin #/aaa/group <group ID>

where

group ID is an integer in the range 1 to 1023 that uniquely identifies the group in the Nortel SNAS domain.

When you first create the group, you must enter the group ID. After you have created the group, you can use either the ID or the name to access the group for configuration.

When you first create the group, you are prompted to enter the following parameters:

- group name—a string that uniquely identifies the group on the Nortel SNAS. The maximum length of the string is 255 characters. After you have defined a name for the group, you can use either the group name or the group ID to access the **Group** menu. The group name must match a group name used by the authentication services. For more information, see Table 22 "Group names in the Nortel SNAS and authentication services" (page 153).
- number of sessions—the maximum number of simultaneous portal or Nortel SNAS sessions allowed for each member of the group. The default is 0 (unlimited). You can later modify the number of sessions by using the **restrict** command on the **Group** menu.

ATTENTION
MAC OSX and Linux OS are supported through filter only mechanism; no VLAN change is possible.

ATTENTION
MAC OSX users must log in again after sleep mode is activated.

The **Group** menu appears.

ATTENTION
If you ran the quick setup wizard during initial setup, a group called nhauser is created with group ID = 1.

The **Group** menu includes the following options:

Table 24
Configuring groups

/cfg/doamin #/aaa/group # **followed by:**	
name <name>	Names or renames the group. After you have defined a name for the group, you can use either the group name or the group ID to access the **Group** menu. • **name** is a string that must be unique in the domain. The maximum length of the string is 255 characters. The group name must match a group name used by the authentication services. For more information, see Table 22 "Group names in the Nortel SNAS and authentication services" (page 153).
restrict	Sets the maximum number of simultaneous portal or Nortel SNAS sessions allowed for each member of the group. For example, if the value is set to 2, then a user can use two computers at the same time and have two simultaneous sessions running. The default is 0 (unlimited).
	Accesses the **Linksets** menu, in order to map preconfigured linksets to the group (see "Mapping linksets to a group or profile" (page 167)). For information about creating and configuring the linksets, see "Configuring linksets" (page 251).
extend <profile ID>	Accesses the **Extended Profiles** menu, in order to configure extended profiles for the group (see "Configuring extended profiles" (page 164)). To view existing profiles, press **TAB** following the **extend** command.

Table 24
Configuring groups (cont'd.)

/cfg/doamin #/aaa/group # **followed by:**	
srs <SRS rule name>	Specifies the preconfigured Nortel Health Agent SRS rule to apply to the group. For information about configuring the SRS rules using the SREM, see *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, . You cannot configure SRS rules in the CLI.
mactrust <bypass | none>	Sets the authentication and integrity checking requirements. Select **bypass** to apply MAC authentication. If the client passes MAC authentication, then portal authentication and Nortel Health Agent integrity checking are bypassed; the client is given access to the network. Since Nortel Health Agent does not run, the system automatically applies Filter_only enforcement (see **enftype** below). If a user belongs to several groups, bypass occurs only when all groups are configured for bypass. If bypass authentication fails, the system invokes portal authentication and Nortel Health Agent integrity checking. The bypass option requires that the MAC address of the end point is registered in the local (Nortel SNAS) MAC database. For information about managing a local MAC database, see "Managing the local MAC database" (page 206). Select **none** to provide portal authentication and integrity checking only.

Table 24
Configuring groups (cont'd.)

/cfg/doamin #/aaa/group # **followed by:**	
agentmode <continuous | runonce | never>	Establishes Nortel Health Agent monitoring mode. Select **continuous** for cyclic monitoring of the end point by Nortel Health Agent. The user must keep the initial browser window open for the duration of the session. Select **runonce** for one cycle of checking only. The user can close the browser after Nortel Health Agent has run and the end point has been moved to the Green zone. **runonce** is applied automatically when the end point operating system is MacOS or Linux. The Nortel Health Agent integrity check is not performed on non-Windows operating systems. Nortel Health Agent does not run when **never** is selected and network access is determined by authentication only. The system proceeds as if the device passed the Nortel Health Agent integrity check. Filter_only enforcement is applied automatically for non-Windows operating systems and when **never** is selected (see **enftype** below).
macreg <true | false>	Provides access to the local MAC database from the client PC. **true** allows group members to add or modify entries; **false** denies access. For information about managing a local MAC database, see "Managing the local MAC database" (page 206).

Table 24
Configuring groups (cont'd.)

/cfg/doamin #/aaa/group # **followed by:**	
enftype <filter-only | vlan-filter>	Establishes the enforcement type for NSNA network access devices; that is, device that support SSCP. **filter-only** indicates that Red, Yellow, and Green enforcement zones are specified by filters within the Red VLAN. **vlan-filter** indicates that enforcement zones are specified by filters applied to unique Red, Yellow, and Green VLANs. For information on enforcement types, see "Nortel SNAS enforcement types" (page 28).
admrights <user> <passwd> <action> <reset>	Sets a username and password for raising the privilege of the Nortel Health Agent applet to administrator; applies to Windows operating systems only. When the **vlan-filter** enforcement type applies, Nortel Health Agent requires administrator privileges to the PC in order to change the IP address of the PC. If the privileges Nortel Health Agent inherits from the username/password of the user do not provide administrator privileges, you can use **admrights** to raise the Nortel Health Agent privileges. Enter an administrator username and password for **user** and **password**, respectively; for example, the network administrator username and password. The **user** field accepts usernames with the format *domain\username*. When the administrator username and password setting are not configured the following actions can be selected: • **no_access** denies access to the network; this is the default • **filter_only** selects filter_only enforcement (see **enftype** above).

Table 24
Configuring groups (cont'd.)

/cfg/doamin #/aaa/group # **followed by:**	
	User access to the network is denied when the administrative rights parameter is active and the username/password configuration is invalid. Use **reset** to remove the admrights username and password; that is, as if they had never been configured.
comment <comment>	Sets a comment for the group.
del	Removes the group from the Nortel SNAS domain. When you delete the group, you also delete all extended profiles associated with that group ID.

Figure 5 "Group menu commands" (page 161) shows sample output for the **/cfg/doamin #/aaa/group <group ID>** command and commands on the **Group** menu.

Figure 5
Group menu commands

```
>> Main# /cfg/domain 1/AAA/group 2
Creating Group 2
Group name: TestGroup
Enter number of sessions (0 is unlimited):

------------------------------------------------------------
[Group 2 Menu]
    name     - Set group name
    restrict - Set number of login sessions
    linkset  - Linkset menu
    extend   - Extended profiles menu
    tgsrs    - Set TunnelGuard SRS Rule
    comment  - Set comment
    del      - Remove group

>> Group 2# tgsrs
Current value: ""
Enter TunnelGuard SRS rule name: TestRule

>> Group 2#
```

Table 25
Configuring group 1

cfg/domain #/aaa/group 1/cachepass	
Usage	cachepass : true|false

Table 26
Configuring group 1

cfg/domain #/aaa/group 1/syscredent/	
User	Set the system username.
passwd	Set the system password.
prevuser	Set the systems previous username.
prevpasswd	Systems previous password.
actdate	New password effective date.
earplush	
exprprev	
updclients	
reset	
ena	
dis	

Configuring client filters

To create and configure a client filter, use the following command:

/cfg/doamin #/aaa/filter <filter ID>

where

filter ID is an integer in the range 1 to 63 that uniquely identifies the filter in the Nortel SNAS domain.

When you first create the filter, you must enter the filter ID. After you have created the filter, you can use either the ID or the name to access the filter for configuration.

When you first create the filter, you are prompted to enter the client filter name.

The **Client Filter** menu appears.

ATTENTION
If you ran the quick setup wizard during initial setup, two client filters have been created: `nha_passed` (filter ID = 1) and `nha_failed` (filter ID = 2).

The **Client Filter** menu includes the following options:

Table 27
Configuring client filters

/cfg/doamin #/aaa/filter <filter ID> **followed by:**	
name <name>	Names or renames the filter. After you have defined a name for the filter, you can use either the filter name or the filter ID to access the **Client Filter** menu. • **name** is a string that must be unique in the domain. The maximum length of the string is 255 characters. You reference the client filter name when configuring the extended profile.
nha **true | false | ignore**	Specifies whether passing or failing the Nortel Health Agent host integrity check triggers the filter. • **true**—the client filter triggers when the Nortel Health Agent check succeeds. • **false**—the client filter triggers when the Nortel Health Agent check fails. • **ignore**—passing or failing the Nortel Health Agent check will not trigger the client filter. The default is **ignore**. For example, in order to grant limited access rights to users who fail the Nortel Health Agent check, set the **nha** value to **false**, create an extended profile that references this client filter, and then map the extended profile to a restrictive VLAN. For information about configuring the Nortel Health Agent checks, see "Configuring the Nortel Health Agent check" (page 92).
comment <comment>	Creates a comment about the client filter.
del	Removes the client filter from the current configuration.

Figure 6 "Client Filter menu commands" (page 164) shows sample output for the **/cfg/doamin #/aaa/filter <filter ID>** command and commands on the **Client Filter** menu.

Figure 6
Client Filter menu commands

```
>> Main# /cfg/domain 1/aaa/filter 1

------------------------------------------------------------
[Client Filter 1 Menu]
      name       - Set filter name
      nha        - Nortel Health Agent checks passed
      nap        - NAP checks passed
      patchlink  - Patchlink checks passed
      comment    - Set comment
      del        - Remove client filter

>> Client Filter 1# nha
Current value: true
Nortel Health checks passed (true/false/ignore): true

>> Client Filter 1# _
```

Configuring extended profiles

To create and configure an extended profile, use the following command:

/cfg/doamin #/aaa/group <group ID | group name> /extend [<profile ID>]

where

profile ID is an integer in the range 1 to 63 that uniquely identifies the profile in the group. If you do not enter the profile ID as part of the command, you are prompted to do so.

When you first create the extended profile, you must enter the profile ID. After you have created the extended profile, you can use either the profile ID or the name of the associated client filter to access the extended profile for configuration.

When you first create the profile, you are prompted to enter the following parameters:

- client filter name—the name of the predefined client filter that determines whether the Nortel SNAS will apply this extended profile to the user. To view available filters, press **TAB** at the prompt. You can later change the filter referenced by the profile by using the **filter** command on the **Extended Profile** menu.
- VLAN—the name of the VLAN to which the Nortel SNAS will assign users with this profile. You can later change the VLAN assignment for the profile by using the **vlan** command on the **Extended Profile** menu.

The **Extended Profile** menu appears.

ATTENTION
If you ran the quick setup wizard during initial setup, two extended profiles have been created: profile ID 1 associated with client filter `nha_failed`, and profile ID 2 associated with client filter `nha_passed`.

The **Extended Profile** menu includes the following options:

Table 28
Configuring profiles

/cfg/doamin #/aaa/group #/extend # **followed by:**	
filter <name>	Specifies the predefined client filter that determines whether the Nortel SNAS will apply this extended profile to the user. If the user's Nortel Health Agent check result matches the filter's criteria, the Nortel SNAS will apply the extended profile. To view available filters, press **TAB** following the **filter** command. • **name** is a string that must be unique in the domain. For information about configuring client filters, see "Configuring client filters" (page 162).
vlan <name>	Specifies the VLAN to which the Nortel SNAS will assign users with this profile. • **name** is a string that must be unique in the domain.
linkset	Accesses the **Linksets** menu, in order to map preconfigured linksets to the profile (see "Mapping linksets to a group or profile" (page 167)). For information about creating and configuring the linksets, see "Configuring linksets" (page 251).
del	Removes the extended profile from the group.

Figure 7 "Extended Profile menu commands" (page 166) shows sample output for the **/cfg/doamin #/aaa/group <group ID> /extend** command and commands on the **Extended Profile** menu.

Figure 7
Extended Profile menu commands

```
>> Main# cfg/domain 1/aaa/group 2/extend
Enter profile number or filter reference name (1-63): 1
Creating Extended Profile 1
Enter client filter name:
tg_failed(2) tg_passed(1)
Enter client filter name: tg_passed
Enter VLAN name: green

------------------------------------------------------------
[Extended Profile 1 Menu]
   filter  - Set client filter reference
   vlan    - Set VLAN name
   linkset - Linkset menu
   del     - Remove profile

>> Extended Profile 1# ../extend 2/filter tg_failed/vlan
yellow
Creating Extended Profile 2

>> Extended Profile 2#
```

Creating RADIUS attributes to a group

To create a RADIUS Attribute to a group, access the **Group RADIUS Attributes** menu from the **Group** menu. Use the following command:

/cfg/doamin #/aaa/group #/radattr

The **Group RADIUS Attributes** menu appears.

The **Group RADIUS Attributes** menu includes the following options:

Table 29
Configure RADIUS Attributes

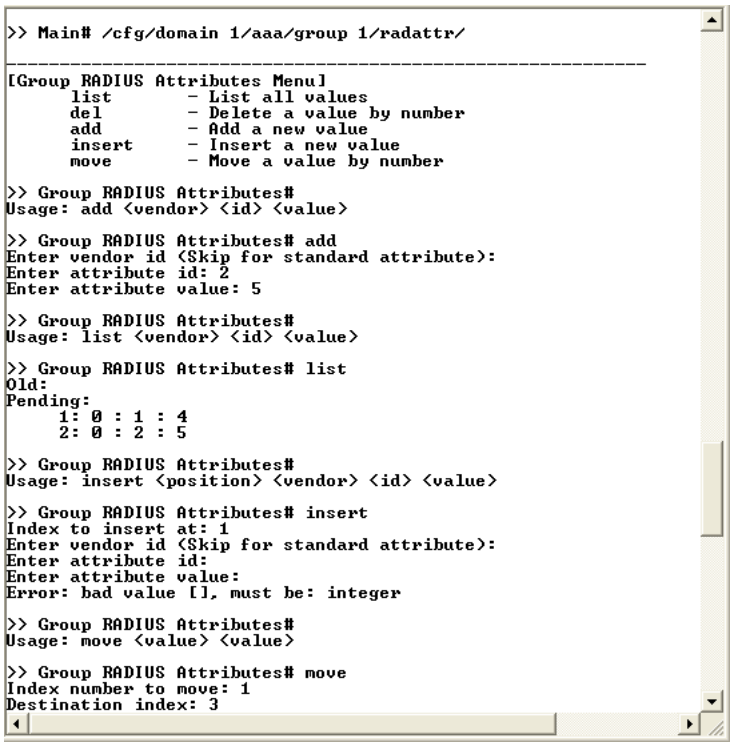
/cfg/doamin #/aaa/group #/radattr **followed by:**	
list <vendor> <id> <value>	Lists the currently configured RADIUS attributes by index number.
del <index>	Removes the RADIUS attribute entry represented by the specified index number. The index numbers of the remaining entries adjust accordingly.
add <vendor> <id> <value>	Adds a RADIUS attribute to the group. You can add as many RADIUS attributes as you want.

Table 29
Configure RADIUS Attributes (cont'd.)

/cfg/doamin #/aaa/group #/radattr **followed by:**	
insert <position> <vendor> <id> <value>	Inserts a RADIUS attribute at a particular position in the list.
move <value> <value>	Moves a RADIUS attribute entry up or down the list. The index numbers of the remaining entries adjust accordingly.

The RADIUS Attribute menu commands shows a sample output for the **/cfg/doamin #/aaa/group <group ID> /radattr** command and commands on the **Group RADIUS Attributes** menu.

Figure 8
Group RADIUS Attribute menu commands



Mapping linksets to a group or profile

You can tailor the portal page for different users by mapping preconfigured linksets to groups and extended profiles.

For more information about linksets, see "Linksets and links" (page 234).

To map a linkset to a group, access the **Linksets** menu from the **Group** menu. Use the following command:

```
/cfg/doamin #/aaa/group #/linkset
```

To map a linkset to an extended profile, access the **Linksets** menu from the **Extended Profile** menu. Use the following command:

```
/cfg/doamin #/aaa/group #/extend #/linkset
```

The **Linksets** menu appears.

The **Linksets** menu includes the following options:

Table 30
Mapping linksets

`/cfg/doamin #/aaa/group #[/extend #]/linkset` **followed by:**	
`list`	Lists the currently configured linksets by index number.
`del <index number>`	Removes the linkset entry represented by the specified index number. The index numbers of the remaining entries adjust accordingly.
`add <linkset name>`	Adds a linkset to the group or extended profile. The linkset on the portal page after the user has been authenticated. You can add as many linksets as you want. The Nortel SNAS assigns an index number to the linkset name as you add the linkset to the list for the group. The linksets display on the portal page in the order of the index numbers.
`insert <index number> <linkset name>`	Inserts a linkset at a particular position in the list. The index numbers of existing linkset entries with this index number and higher are incremented by 1.
`move <index number> <new index number>`	Moves a linkset entry up or down the list. The index numbers of the remaining entries adjust accordingly.

Figure 9 "Linksets menu commands" (page 169) shows a sample output for the `/cfg/doamin #/aaa/group <group ID> /linkset` command and commands on the **Linksets** menu.

Figure 9
Linksets menu commands

```
>> Main# cfg/domain 1/aaa/group 1/linkset

------------------------------------------------------------
[Linksets Menu]
    list      - List all values
    del       - Delete a value by number
    add       - Add a new value
    insert    - Insert a new value
    move      - Move a value by number

>> Linksets# add
linkset name: example1

>> Linksets# add example2

>> Linksets# list
Old:
Pending:
     1: example1
     2: example2

>> Linksets# insert 2 example3

>> Linksets# list
Old:
Pending:
     1: example1
     2: example3
     3: example2

>> Linksets# move
Index number to move: 3
Destination index: 1

>> Linksets# list
Old:
Pending:
     1: example2
     2: example1
     3: example3

>> Linksets# del 2

>> Linksets# list
Old:
Pending:
     1: example2
     2: example3
```

Creating a default group

To create a default group, first create a group with extended profiles mapped to a restrictive VLAN (see “Configuring groups” (page 156) and “Configuring extended profiles” (page 164)). Then use the following command to make this group the default group:

/cfg/doamin #/aaa/defgroup <group name>

Configuring authentication

This chapter includes the following topics:

Overview

The Nortel SNAS controls authentication of clients when they log on to the network.

The Nortel SNAS supports the following authentication methods in Nortel Secure Network Access Switch Software Release 1.6.1:

- external databases
  - Remote Authentication Dial-In User Service (RADIUS)
  - Lightweight Directory Access Protocol (LDAP)
- local databases on the Nortel SNAS
  - local portal database
  - local MAC database

ATTENTION
If you ran the quick setup wizard during initial setup, the Local database authentication method has been created as Authentication 1.

You can configure more than one authentication method within a Nortel SNAS domain. You determine the order in which the methods are applied by default. Client credentials are checked against the various authentication databases until the first match is found.

You can configure the methods so that their names display on the portal login page (see "Configuring authentication methods" (page 177)). You can then direct clients to select a specific authentication server (for example, for direction to a specific Windows domain). If the client selects a Login Service name, the authentication request is directed immediately to the specified service. Otherwise, authentication defaults to being carried out according to the authentication order you have configured (see "Specifying authentication fallback order" (page 209)).

For general information about authentication within the Nortel SNAS, see *Nortel Secure Network Access Solution Guide*, (NN47230-200).

Before you begin

Before you configure authentication on the Nortel SNAS, you must complete the following tasks:

Step	Action
1	Create the Nortel SNAS domain, if applicable (see "Creating a domain" (page 83)). If you ran the quick setup wizard during initial setup, doamin # has been created on the Nortel SNAS. **ATTENTION** With Nortel Secure Network Access Switch Software Release 1.6.1, you cannot configure the Nortel SNAS to have more than one domain.
2	Create and configure the groups (see "Configuring groups and profiles" (page 149)).
3	For external authentication servers, create or modify settings on the external server as required. **a** A free RADIUS server may require specific settings in the clients.conf file and the Users file to match group parameters you may have configured on the Nortel SNAS. **b** A Steel-belted RADIUS server requires specific settings in the vendor.ini file, master dictionary, and vendor dictionary.

c An MS IAS RADIUS server may require vendor parameters to be configured on the Microsoft Management Console (MMC).

4 To configure external authentication, you require the following information about the authentication server configuration:

a RADIUS servers:

- server IP address
- port number used for the service
- shared secret
- Vendor-Id attribute
- Vendor-Type

ATTENTION

You can assign vendor-specific codes to the Vendor-Id and Vendor-Type attributes. The RADIUS server uses Vendor-Id and Vendor-Type attributes in combination to identify what values it will assign and send for attributes such as group name and session timeout.

Each vendor has a specific dictionary. The Vendor-Id specified for an attribute identifies the dictionary the RADIUS server will use to retrieve the attribute value. The Vendor-Type indicates the index number of the required entry in the dictionary file.

The Internet Assigned Numbers Authority (IANA) has designated SMI Network Management Private Enterprise Codes that can be assigned to the Vendor-Id attribute (see http://www.iana.org/assignments/enterprise-numbers).

RFC 2865 describes usage of the Vendor-Type attribute.

If you specify Vendor-Id and Vendor-Type on the RADIUS server and on the Nortel SNAS, the Nortel SNAS will retrieve vendor-specific values for the associated attribute. If you set the Vendor-Id and Vendor-Type attributes to 0, the RADIUS server sends standard attribute values.

b LDAP servers:

- server IP address
- port number used for the service
- configured accounts and users so that you can specify appropriate search entries and group and user attributes

--End--

Configuring authentication

The basic steps for configuring and managing client authentication are:

Step	Action
1	Create the authentication methods.
2	Configure specific settings for the methods.
3	Specify the order in which the authentication methods will be applied. Perform this step even if you define only one method on the Nortel SNAS.

--End--

To configure authentication, access the **AAA** menu by using the following command:

```
/cfg/doamin #/aaa
```

From the **AAA** menu, you can manage the following authentication-related tasks:

- creating and configuring the authentication methods
  - “Configuring authentication methods” (page 177)
  - “Configuring advanced settings” (page 179)
  - “Configuring RADIUS authentication” (page 180)
  - “Configuring LDAP authentication” (page 187)
  - “Configuring local database authentication” (page 200)
- setting the order in which authentication methods will be applied (see “Specifying authentication fallback order” (page 209))

Roadmap of authentication commands

The following roadmap lists the CLI commands to configure client authentication in the Nortel SNAS domain. Use this list as a quick reference or click on any entry for more information:

Table 31
Roadmap of CLI commands

Command	Parameter
`/cfg/doamin #/aaa/auth <auth ID>`	`type radius | ldap | local`
	`name <name>`
	`display`

Table 31
Roadmap of CLI commands (cont'd.)

Command	Parameter
	del
/cfg/doamin #/aaa/auth #/adv	groupauth <auth IDs>
	secondauth <auth ID>
/cfg/doamin #/aaa/auth #/radius	vendorid <vendor ID>
	vendortype <vendor type>
	domainid <domain ID>
	domaintype <domain type>
	authproto pap|chapv2
	timeout <interval>
/cfg/doamin #/aaa/auth #/radius/servers	list
	del <index number>
	add <IPaddr> <port> <shared secret>
	insert <index number> <IPaddr>
	move <index number> <new index number>
/cfg/doamin #/aaa/auth #/radius/sessiontim	vendorid <vendor ID>
	vendortype <vendor type>
	ena
	dis
/cfg/doamin #/aaa/auth #/ldap	searchbase <DN>
	groupattr <names>
	userattr <names>
	isdbinddn <DN>
	isdbindpas <password>
	enaldaps true | false
	ldapscert
	enauserpre true | false
	enacutdomain true | false
	enashortgrp true | false
	timeout <interval>
/cfg/doamin #/aaa/auth #/ldap/servers	list
	del <index number>

Table 31
Roadmap of CLI commands (cont'd.)

Command	Parameter
	add <IPaddr> <port>
	insert <index number> <IPaddr>
	move <index number> <new index number>
/cfg/doamin #/aaa/auth #/ldap/ldapmacro	list
	del <index number>
	add <variable name> <LDAP attribute> [<prefix>] [<suffix>]
	insert <index number> <variable name>
	move <index number> <new index number>
/cfg/doamin #/aaa/auth #/ldap/activedire	enaexpired true | false
	expiredgro <group>
	recursivem true | false
/cfg/doamin #/aaa/auth #/ldap/adv	enaxfilter true | false
	xfilteratt <filter attribute name>
	xfilterval <filter attribute value>
/cfg/doamin #/aaa/auth #/local	add <user name> <password> <group>
	passwd <user name> <password>
	groups <user name> <desired group>
	del <user name>
	list
	import <protocol> <server> <filename> <key>
	export <protocol> <server> <filename> <key>
/cfg/doamin #/aaa/auth #/local/radattr	add <user name> <vendor id> <attribute id> <attribute value>
	del <user name>
	list
/cfg/doamin #/aaa/macdb	add
	del <MAC address>
	list
	show <MAC address>
	import <protocol> <server> <filename>

Table 31
Roadmap of CLI commands (cont'd.)

Command	Parameter
	`export <protocol> <server> <filename>`
	`clear`
`/cfg/doamin #/aaa/authorder <auth ID>[,<auth ID>]`	

Configuring authentication methods

To create and configure an authentication method, use the following command:

```
/cfg/doamin #/aaa/auth <auth ID>
```

where

auth ID is an integer in the range 1 to 63 that uniquely identifies the authentication method in the Nortel SNAS domain.

When you first create the method, you are prompted to specify the type. For Nortel Secure Network Access Switch Software Release 1.6.1, valid options are:

- RADIUS
- LDAP
- local

The selected method type determines the remainder of the parameters you are prompted to provide when you create the method, as well as the submenu options that are provided on the **Authentication** menu appears.

The **Authentication** menu includes the following options:

Table 32
Configuring Authentication

`/cfg/doamin #/aaa/auth <auth ID>` **followed by:**	
`type radius|ldap|ntlm|siteminder|cleartrust|cert|rsa|local`	Sets the authentication mechanism. **ATTENTION** The selected authentication type determines, which submenu option will display.

Table 32
Configuring Authentication (cont'd.)

/cfg/doamin #/aaa/auth <auth ID> **followed by:**	
name <name>	Names or renames the method. After you have defined a name for the method, you can use either the method name or the `auth ID` to access the **Authentication** menu. • **name** is a string that must be unique in the domain. The maximum allowable length of the string is 255 characters, but Nortel recommends a maximum of 32 characters. In future releases of the Nortel SNAS software, you will be able to reference this string in a client filter, so that authentication to the server in question becomes a condition for access rights for a group.
display	Specifies a name for the method, to display in the Login Service list box on the portal login page, together with the names of other authentication services available.
radius | ldap | local	Accesses a method-specific menu, in order to configure settings for the method. The option displayed depends on the method type. • `radius`—accesses the **RADIUS** menu (see "Configuring RADIUS authentication" (page 180)) • `ldap`—accesses the **LDAP** menu (see "Configuring LDAP authentication" (page 187)) • `local`—accesses the **Local database menu** (see "Configuring local database authentication" (page 200))
adv	Accesses the **Advanced** menu, in order to configure the current method to retrieve group information from other authentication schemes (see "Configuring advanced settings" (page 179)).
del	Removes the method from the Nortel SNAS domain.

Configuring advanced settings

You can configure the Nortel SNAS domain to use one method for authentication and another for authorization.

For example, there are three authentication methods configured for the domain: Local (auth ID 1), RADIUS (auth ID 2), and LDAP (auth ID 3). The user groups are stored in an LDAP database. You can configure the domain to have the Local and LDAP methods used for authorization after users have been authenticated by RADIUS. In this example, the command is: **`/cfg/doamin #/aaa/auth #/adv/groupauth 1,3`**. When a user logs on through RADIUS, the system first checks the RADIUS database. If no match is found, the system checks the other authentication schemes (in the order in which you listed them in the **`groupauth`** command) to see if the user name can be matched against user groups defined in the authentication databases. The first group matched is returned to the Nortel SNAS as the user's group, and determines the user's access privileges for the session.

To configure the current authentication scheme to retrieve user group information from a different authentication scheme, use the following command:

`/cfg/doamin #/aaa/auth #/adv`

The **Advanced** menu appears.

The **Advanced** menu includes the following options:

Table 33
Configuring Advance Settings

`/cfg/doamin #/aaa/auth #/adv` **followed by:**	
`groupauth <auth IDs>`	Specifies one or more preconfigured LDAP or Local database authentication schemes (not including the current one) that will be used to retrieve the user's group information after the user has been authenticated. To specify more than one authentication method to use for authorization, enter the auth IDs separated by a comma (,).
`secondauth <auth ID>`	Specifies a second authentication service to be used after the first one succeeds. The feature supports single sign-on to backend

/cfg/doamin #/aaa/auth #/adv **followed by:**	
	servers in cases where the first authentication method is token based or uses client certificate authentication. **ATTENTION** Not supported in Nortel Secure Network Access Switch Software Release 1.6.1.

Configuring RADIUS authentication

To configure the Nortel SNAS domain to use an external RADIUS server for authentication, use the following command:

/cfg/doamin #/aaa/auth <auth ID>

where **auth ID** is an integer in the range 1 to 63 that uniquely identifies the authentication method in the Nortel SNAS domain. If you do not specify the `auth ID` in the command, you are prompted for it.

When you first create the method for the domain, you must enter the authentication ID. After you have created the method and defined a name for it, you can use either the ID or the name to access the method for configuration.

You can perform the following configuration tasks:

- “Adding the RADIUS authentication method” (page 181)
- “Modifying RADIUS configuration settings” (page 182)
- “Managing RADIUS authentication servers” (page 184)
- “Configuring session timeout” (page 186)

Adding the RADIUS authentication method

The command to create the authentication ID launches a wizard. When prompted, enter the following information. You can later modify all settings for the specific RADIUS configuration (see "Configuring authentication methods" (page 177) and "Modifying RADIUS configuration settings" (page 182)).

- authentication type—options are **radius**|**ldap**|**ntlm**|**sitemeinder**|**cleartrust**|**cert**|**rsa**|**local**. Enter **radius**.
- authentication method name (`auth name`)—a string that specifies a name for the method. After you have defined a name for the method, you can use either the method name or the `auth ID` to access the **Authentication** menu. In future releases of the Nortel SNAS software, you will be able to reference this string in a client filter, so that authentication to the server in question becomes a condition for access rights for a group.
- IP address of the RADIUS server.
- port on which the RADIUS server is listening—the port number configured on the RADIUS server to specify the port used by the service. The default is 1812.
- shared secret—a unique shared secret configured on the RADIUS server that authenticates the Nortel SNAS to the RADIUS server.
- vendor ID for group—corresponds to the vendor-specific attribute used by the RADIUS server to send group names to the Nortel SNAS. The default Vendor-Id is 1872 (Alteon).
  To use a standard RADIUS attribute rather than the vendor-specific one, set the vendor ID to 0 (see also vendor type).
- vendor type for group—corresponds to the Vendor-Type value used in combination with the Vendor-Id to identify the groups to which the user belongs. The group names to which the vendor-specific attribute points must match names you define on the Nortel SNAS using the **/cfg/doamin #/aaa/group <group ID>** command (see "Configuring groups" (page 156)). The default is 1.
  If you set the vendor ID to 0 in order to use a standard RADIUS attribute (see vendor ID), set the vendor type to a standard attribute type as defined in RFC 2865. For example, to use the standard attribute Class, set the vendor ID to 0 and the vendor type to 25.
- vendor ID for domain—corresponds to the vendor-specific attribute used by the RADIUS server to send domain names to the Nortel SNAS. The default Vendor-Id is 1872 (Alteon).
- vendor type for domain—corresponds to the Vendor-Type value used in combination with the Vendor-Id to identify the domain. The default is 3.

The **Authentication** menu .

Figure 10 "Authentication menu commands—RADIUS" (page 182) shows sample output for the RADIUS method for the **/cfg/doamin #/aaa/auth <auth ID>** command and commands on the **Authentication** menu.

Figure 10
Authentication menu commands—RADIUS

```
>> Main# /cfg/domain 1/aaa/auth
Enter auth id: (1-63) 2
Creating Authentication 2
Select one of radius, ldap or local: radius
Auth name: radius
Entering: RADIUS settings menu
Entering: RADIUS servers menu
IP Address to add: <IPaddr>
Port (default is 1812):
Enter shared secret: <secret>
Leaving: RADIUS servers menu
Enter vendor id for group [alteon]:
Enter vendor type for group [1]:
Enter vendor id for domain [alteon]:
Enter vendor type for domain [3]:
Leaving: RADIUS settings menu

------------------------------------------------------------
[Authentication 2 Menu]
   type     - Set authentication mechanism
   name     - Set auth name
   display  - Set auth display name
   radius   - RADIUS settings menu
   adv      - Advanced settings menu
   del      - Remove Authentication

>> Authentication 2#
```

Modifying RADIUS configuration settings

To modify settings for the authentication method itself, see “Configuring authentication methods” (page 177).

To modify settings for the specific RADIUS configuration, use the following command:

/cfg/doamin #/aaa/auth #/radius

The **RADIUS** menu appears.

The **RADIUS** menu includes the following options:

Table 34
Configuring authentication methods

/cfg/doamin #/aaa/auth #/radius **followed by:**	
servers	Accesses the **RADIUS servers** menu, in order to manage the external RADIUS servers configured for the domain (see "Managing RADIUS authentication servers" (page 184)).
vendorid <vendor ID>	Specifies the vendor-specific attribute used by the RADIUS server to send group names to the Nortel SNAS. The default Vendor-Id is 1872 (Alteon). To use a standard RADIUS attribute rather than the vendor-specific one, set the vendor ID to 0 (see also vendor type). **ATTENTION** If **authproto** is **chapv2**, the Vendor-Id must be set to 311 (Microsoft).
vendortype <vendor type>	Specifies the Vendor-Type value used in combination with the Vendor-Id to identify the groups to which the user belongs. The group names to which the vendor-specific attribute points must match names you define on the NSNAS. The default is 1. If you set the vendor ID to 0 in order to use a standard RADIUS attribute (see vendor ID), set the vendor type to a standard attribute type as defined in RFC 2865. For example, to use the standard attribute Class, set the vendor ID to 0 and the vendor type to 25.
domainid <domain ID>	Specifies the vendor-specific attribute used by the RADIUS server to send domain names to the NSNAS. The default Vendor-Id is 1872 (Alteon). **ATTENTION** If **authproto** is **chapv2**, consider setting the Vendor-Id for the domain to 10 (MS-CHAP-Domain).

Table 34
Configuring authentication methods (cont'd.)

/cfg/doamin #/aaa/auth #/radius **followed by:**	
domaintype <domain type>	Specifies the Vendor-Type value used in combination with the Vendor-Id to identify the domain. The default is 3.
authproto pap | chapv2	Specifies the protocol used for communication between the Nortel SNAS and the RADIUS server. The options are: • **pap**—Password Authentication Protocol (PAP) • **chapv2**—Challenge Handshake Authentication Protocol (CHAP), version 2 The default is PAP.
timeout <interval>	Sets the timeout interval for a connection request to a RADIUS server. At the end of the timeout period, if no connection has been established, authentication will fail. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), or hours (h). If you do not specify a measurement unit, seconds is assumed. The range is 1–10000 seconds. The default is 10 seconds.
sessiontim	Accesses the **Session Timeout** menu, in order to configure settings to control the length of client sessions (see "Configuring session timeout" (page 186)).

Managing RADIUS authentication servers

You can configure additional RADIUS servers for the domain, for redundancy. You can have a maximum of three RADIUS authentication servers in the configuration. You can control the order in which the RADIUS servers respond to authentication requests.

To enable RADIUS authentication, ensure that the authentication ID that represents the RADIUS configuration is included in the authentication order you have specified for the Nortel SNAS domain (see "Specifying authentication fallback order" (page 209)).

To manage the RADIUS servers used for client authentication in the domain, use the following command:

/cfg/doamin #/aaa/auth #/radius/servers

The **Radius servers** menu appears.

The **Radius servers** menu includes the following options:

Table 35
RADIUS authenticaion servers

/cfg/doamin #/aaa/auth #/radius/servers **followed by:**	
list	Lists the IP address, port, and shared secret of currently configured RADIUS authentication servers, by index number.
del <index number>	Removes the specified RADIUS authentication server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured RADIUS authentication servers, use the **list** command.
add <IPaddr> <port> <shared secret>	Adds a RADIUS authentication server to the configuration. You are prompted to enter the following information: • **IPaddr**—the IP address of the authentication server • **port**—the TCP port number used for RADIUS authentication. The default is 1813. • **shared secret**—the password used to authenticate the Nortel SNAS to the authentication server The system automatically assigns the next available index number to the server.

Table 35
RADIUS authenticaion servers (cont'd.)

/cfg/doamin #/aaa/auth #/radius/servers **followed by:**	
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of RADIUS authentication servers in the configuration. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the authentication server you are adding The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of RADIUS authentication servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

Configuring session timeout

You can configure the Nortel SNAS to enable session timeout and to retrieve a session timeout value from the RADIUS server. With session timeout enabled, the session timeout value controls the length of the client's Nortel SNAS network session. When the time is up, the client is automatically logged out. Idle time has no effect on the session timeout.

To configure the Nortel SNAS for session timeout, use the following command:

/cfg/doamin #/aaa/auth #/radius/sessiontim

The **Session Timeout** menu appears.

The **Session Timeout** menu includes the following options:

Table 36
Configuring session timeout

/cfg/doamin #/aaa/auth #/radius/sessiontim **followed by:**	
vendorid <vendor ID>	Specifies the vendor-specific attribute used by the RADIUS server to send a session timeout value to the Nortel SNAS. The default Vendor-Id is 0. With the Vendor-Type also set to 0 (the default value), the RADIUS server sends the standard attribute for session timeout.
vendortype <vendor type>	Specifies the Vendor-Type value used in combination with the Vendor-Id to identify the session timeout value to send to the Nortel SNAS. The default is 0.
ena	Enables retrieval of the RADIUS server session timeout value. The default is disabled.
dis	Disables retrieval of the RADIUS server session timeout value. The default is disabled.

Configuring LDAP authentication

To configure the Nortel SNAS domain to use an external LDAP server for authentication, use the following command:

/cfg/doamin #/aaa/auth <auth ID>

where **auth ID** is an integer in the range 1 to 63 that uniquely identifies the authentication method in the Nortel SNAS domain. If you do not specify the **auth ID** in the command, you are prompted for it.

When you first create the method for the domain, you must enter the authentication ID. After you have created the method and defined a name for it, you can use either the ID or the name to access the method for configuration.

You can perform the following configuration tasks:

- “Adding the LDAP authentication method” (page 188)
- “Modifying LDAP configuration settings” (page 189)
- “Managing LDAP authentication servers” (page 193)
- “Managing LDAP macros” (page 195)
- “Managing Active Directory passwords” (page 198)

Adding the LDAP authentication method

The command to create the authentication ID launches a wizard. When prompted, enter the following information. For more information about the parameters, see searchbase <DN>. You can later modify all settings for the specific LDAP configuration (see "Configuring authentication methods" (page 177) and "Modifying LDAP configuration settings" (page 189)).

- authentication type—options are **`radius`**|**`ldap`**|**`local`**. Enter **`ldap`**.
- authentication method name (**`auth name`**)—a string that specifies a name for the method. After you have defined a name for the method, you can use either the method name or the **`auth ID`** to access the **Authentication** menu. In future releases of the Nortel SNAS software, you will be able to reference this string in a client filter, so that authentication to the server in question becomes a condition for access rights for a group.
- IP address of the LDAP server.
- port on which the LDAP server is listening—the port number configured on the LDAP server to specify the port used by the service. The default is 389.
- search base entry—the Distinguished Name (DN) that points to one of the following:
  - the entry that is one level up from the user entries (does not require isdBindDN and isdBindPassword)
  - if user entries are located in several places in the LDAP Dictionary Information Tree (DIT), the position in the DIT from where all user records can be found with a subtree search (requires isdBindDN and isdBindPassword)
- group attribute name—the LDAP attribute that contains the names of the groups. You can specify more than one group attribute name.
- user attribute name—refers to one of the following:
  - the LDAP attribute that contains the user name (does not require isdBindDN and isdBindPassword)
  - the LDAP attribute that is used in combination with the user's login name to search the DIT (requires isdBindDN and isdBindPassword)
- isdBindDN—used to authenticate the Nortel SNAS to the LDAP server, so that the LDAP DIT can be searched. The `isdBindDN` corresponds to an entry created in the Schema Admins account (for example, `cn=ldap ldap, cn=Users, dc=example, dc=com`). An account must be created on the LDAP server to enable the Nortel SNAS to do the bind search in the directory structure.

- isdBindPassword—used to authenticate the Nortel SNAS to the LDAP server. The `isdBindPassword` is the password, configured in the Schema Admins account, for the entry referenced in isdBindDN.
- enable LDAPS—if true, makes LDAP requests between the Nortel SNAS and the LDAP server occur over a secure SSL connection. The default is false. Retain the default value or reset to **`false`**.

The **Authentication** menu .

Figure 11 "Authentication menu commands —LDAP" (page 189) shows sample output for the LDAP method for the **`/cfg/doamin #/aaa/auth <auth ID>`** command and commands on the **Authentication** menu.

Figure 11
Authentication menu commands —LDAP

```
>> Main# /cfg/domain 1/aaa/auth
Enter auth id: (1-63) 3
Creating Authentication 3
Select one of radius, ldap, or local: ldap
Auth name: ldap
Entering: LDAP settings menu
Entering: LDAP servers menu
IP Address to add: <IPaddr>
Port (default is 389):
Leaving: LDAP servers menu
Search Base Entry: <search base entry>
Group attribute name: <attribute>
User attribute name: <attribute>
isdBindDN: <DN>
isdBindPassword: <password>
Enable LDAPS (true/false):
Leaving: LDAP settings menu

------------------------------------------------------------
[Authentication <auth ID> Menu]
   type     - Set authentication mechanism
   name     - Set auth name
   display  - Set auth display name
   domain   - Set windows domain for backend single sign-on
   ldap     - LDAP settings menu
   adv      - Advanced settings menu
   del      - Remove Authentication

>> Authentication 3#
```

Modifying LDAP configuration settings

To modify settings for the authentication method itself, see “Configuring authentication methods” (page 177).

To modify settings for the specific LDAP configuration, use the following command:

`/cfg/doamin #/aaa/auth #/ldap`

The **LDAP** menu appears.

The **LDAP** menu includes the following options:

Table 37
Configuring LDAP settings

`/cfg/doamin #/aaa/auth #/ldap` **followed by:**	
`servers`	Accesses the **LDAP servers** menu, in order to manage the external LDAP servers configured for the domain (see "Managing LDAP authentication servers" (page 193)).
`searchbase`	Sets the search base entry.
`groupattr <names>`	Specifies the LDAP attribute that contains the names of the groups. The group names contained in the LDAP attribute must be defined in the Nortel SNAS domain (see "Configuring groups" (page 156)). To specify more than one group attribute name, enter the names separated by a comma (,).
`userattr <names>`	Refers to one of the following: 1. the LDAP attribute that contains the user name used for authenticating a client in the domain The default user attribute name is `uid`. Do not use the **`isdbinddn`** and **`isdbindpas`** commands. 2. if the client's portal logon name is different from the RDN (for example, when using LDAP for authentication towards Active Directory), the LDAP attribute that is used in combination with the client's logon name to search the DIT For example, a user record in Active Directory is defined as the following DN: `cn=Bill Smith, ou=Users, dc=example, dc=com`. The user record also contains the attribute `sAMAccountName=bill`. The user's

Table 37
Configuring LDAP settings (cont'd.)

/cfg/doamin #/aaa/auth #/ldap **followed by:**	
	login name is `bill`. If the user attribute is defined as `sAMAccountName`, the user record for Bill Smith will be found. The **`isdbinddn`** and **`isdbindpas`** parameters are required so that the Nortel SNAS can authenticate itself to the LDAP server, in order to search the DIT.
`isdbinddn <DN>`	Specifies an entry in the LDAP server used to authenticate the Nortel SNAS to the LDAP server, so that the LDAP DIT can be searched. The `isdBindDN` corresponds to an entry created in the Schema Admins account (for example, `cn=ldap ldap, cn=Users, dc=example, dc=com`). Required for `searchbase` and `userattr` method 2.
`isdbindpas <password>`	Specifies the password used to authenticate the Nortel SNAS to the LDAP server. The `isdbindpas` is the password, configured in the Schema Admins account, for the entry referenced in `isdBindDN`. Required for `searchbase` and `userattr` method 2.
`ldapmacro`	Accesses the **LDAP Macro** menu, in order to manage macros (see "Managing LDAP macros" (page 195)).
`enaldaps true` | **`false`**	If true, makes LDAP requests between the Nortel SNAS and the LDAP server occur over a secure SSL connection (LDAPS). The default is false. Retain the default value or reset to **`false`**. **ATTENTION** The default TCP port number used by the LDAP protocol is 389. If LDAPS is enabled, change the port number to 636.

Table 37
Configuring LDAP settings (cont'd.)

/cfg/doamin #/aaa/auth #/ldap **followed by:**	
ldapscert	Specify the certificate number.
enauserpre true | false	Enables or disables storage of user preferences in an external LDAP/Active Directory database. • **true**—storage and retrieval of user preferences is enabled. When the client logs out from a portal session, the Nortel SNAS saves any user preferences accumulated during the session in the isdUserPrefs attribute. The next time the client successfully logs on through the portal, the Nortel SNAS retrieves the LDAP attribute from the LDAP database. • **false**—storage and retrieval of user preferences is disabled. To support storage and retrieval of user preferences, you must extend the LDAP server schema with one new ObjectClass and one new Attribute. For more information, see "Adding User Preferences attribute to Active Directory" (page 485). The default is false.
enacutdomain true | false	Enables or disables the cut domain from the user name.
timeout <interval>	Sets the timeout interval for a connection request to an LDAP server. At the end of the timeout period, if no connection has been established, authentication will fail. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), or hours (h). If you do not specify a measurement unit, seconds is assumed. The range is 1–10000 seconds. The default is 5 seconds.
activedire	Accesses the **Active Directory** menu, in order to manage client passwords (see "Managing Active Directory passwords" (page 198)).

Table 37
Configuring LDAP settings (cont'd.)

`/cfg/doamin #/aaa/auth #/ldap` **followed by:**	
`enashortgr`	Enables the short group format. Configures the NVG to extract the first part of a returned Distinguished Name (DN) as the group name to be used. This makes it easier to configure the group name in the VPN to configure the entire DN string as group name.
`groupsearc`	the LDAP Group Search menu.
`adv`	the Advanced LDAP menu.

Managing LDAP authentication servers

You can configure additional LDAP servers for the domain, for redundancy. You can have a maximum of three LDAP authentication servers in the configuration. You can control the order in which the LDAP servers respond to authentication requests.

If there is more than one LDAP server configured for the Nortel SNAS domain, the first accessible LDAP server in the list returns a reply to the query. This stops the query, regardless of whether or not the client's credentials were matched. If you add more than one LDAP server to the domain, for redundancy, ensure that each listed LDAP server contains the same SSL domain client database.

If the Nortel SNAS clients are dispersed in different LDAP server databases, you can configure the LDAP servers as separate authentication methods, with different authentication IDs. If you include all LDAP authentication IDs in the authentication order, each LDAP server will be used to authenticate client groups.

To enable LDAP authentication, ensure that the authentication ID that represents the LDAP configuration is included in the authentication order you have specified for the Nortel SNAS domain (see "Specifying authentication fallback order" (page 209)).

To manage the LDAP servers used for client authentication in the domain, use the following command:

`/cfg/doamin #/aaa/auth #/ldap/servers`

The **LDAP servers** menu appears.

The **LDAP servers** menu includes the following options:

Table 38
Managing LDAP authentication servers

/cfg/doamin #/aaa/auth #/ldap/servers **followed by:**	
list	Lists the IP address and port of currently configured LDAP servers, by index number.
del <index number>	Removes the specified LDAP server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured LDAP servers, use the **list** command.
add <IPaddr> <port>	Adds an LDAP server to the configuration. You are prompted to enter the following information: • **IPaddr**—the IP address of the authentication server • **port**—the TCP port number used for LDAP authentication. The default is 389. The system automatically assigns the next available index number to the server. **ATTENTION** The default TCP port number used by the LDAP protocol is 389. If LDAPS is enabled, change the port number to 636.
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of LDAP servers in the configuration. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the server you are adding

Table 38
Managing LDAP authentication servers (cont'd.)

/cfg/doamin #/aaa/auth #/ldap/servers **followed by:**	
	The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of LDAP servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

Managing LDAP macros

You can create your own macros (or variables), to allow you to retrieve data from the LDAP database. You can then map the variable to an LDAP user attribute in order to create user-specific links on the portal Home tab. When the client successfully logs on, the variable expands to the value retrieved from the LDAP or Active Directory user record. For more information about using macros in portal links, see "Macros" (page 235).

To configure LDAP macros, use the following command:

/cfg/doamin #/aaa/auth #/ldap/ldapmacro

The **LDAP macro** menu appears.

The **LDAP macro** menu includes the following options:

Table 39
Managing LDAP macros

/cfg/doamin #/aaa/auth #/ldap/ldapmacro **followed by:**	
list	Lists all macros in the LDAP configuration in the Nortel SNAS domain, by index number.

Table 39
Managing LDAP macros (cont'd.)

/cfg/doamin #/aaa/auth #/ldap/ldapmacro **followed by:**	
del <index number>	Removes the specified LDAP macro from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured LDAP macros, use the **list** command.
add <variable name> <LDAP attribute> [<prefix>] [<suffix>]	Adds an LDAP macro to the configuration. You are prompted to enter the following information: • **variable name**—the name of the variable. • **LDAP attribute**—the LDAP user attribute whose value will be retrieved from the client's LDAP/Active Directory user record. • **prefix**—if the value string of the LDAP attribute is long and you wish to extract only part of it, the values at the start of the string that you want to ignore. Combine with a suffix if the value you want is in the middle of the string. • **suffix**—if the value string of the LDAP attribute is long and you wish to extract only part of it, the values at the end of the string that you want to ignore. Combine with a prefix if the value you want is in the middle of the string. The system automatically assigns the next available index number to the macro.
insert <index number> <variable name>	Inserts a macro at a particular position in the list of LDAP macros in the configuration. • **index number**—the index number you want the macro to have • **variable name**—the LDAP macro you are adding

Table 39
Managing LDAP macros (cont'd.)

/cfg/doamin #/aaa/auth #/ldap/ldapmacro **followed by:**	
	The index number you specify must be in use. The index numbers of existing macros with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a macro up or down the list of macros in the configuration. • **index number**—the original index number of the macro you want to move • **new index number**—the index number representing the new position of the macro in the list The index numbers of the remaining entries adjust accordingly.

Group Search Configuration

The LDAP Group Search menu lets you configure the NVG to find group information.

The **Group Search** menu includes the following options:

Table 40
Group Search Configuration

cfg/domain #/aaa/auth #/ldap/groupsearch followed by:	
groupbase **<group searchbase entry>**	Sets the group base search entry Assigns the DN (Distinguished Name) that points to the entry where to start searching for group entries in the Dictionary Information Tree (DIT) on the iPlanet Directory Server The group should be defined in the VPN with one or more access rules.

Table 40
Group Search Configuration (cont'd.)

memberattr	Defines the LDAP attribute that has the group member's name. The default value is **uniqueMember.**
ena	Enables the group search feature.
dis	Disables the group search feature.

Managing Active Directory passwords

You can set up a mechanism for clients to change their passwords when the passwords expire.

Step	Action
1	Define a user group in the Local database for users whose passwords have expired.
2	Create a linkset and link to a site where the user can change the password (see "Configuring groups" (page 156)).
3	Map the linkset to the group (see "Mapping linksets to a group or profile" (page 167)).
4	Set the Active Directory settings using the **/cfg/doamin #/aaa/auth #/ldap/activedire** command.

--End--

To manage clients whose passwords have expired or who need to change their passwords, use the following command:

/cfg/doamin #/aaa/auth #/ldap/activedire

The **Active Directory Settings** menu appears.

The **Active Directory Settings** menu includes the following options:

Table 41
Managing Active Directory passwords

/cfg/doamin #/aaa/auth #/ldap/activedire **followed by:**	
enaexpired true | false	Specifies whether the system will perform a password-expired check. • **true**—the system performs a password-expired check against Active Directory when the client logs on. • **false**—the system does not perform a password-expired check against Active Directory when the client logs on.
expiredgro <group>	Specifies the group in which clients with expired passwords will be placed.
expasgrou	Sets the group in which users with expired passwords should be placed. Before using this command, define the use group in the Local database. Configure a link to a site where the user can change his/her password. Configure an access rule restricting access to the specified site.
recursivem true | false	Specifies the setting for recursive group membership. • **true**—if the client belongs to an Active Directory group which, in turn, belongs to another group, all groups are returned. • **false**—if the client belongs to an Active Directory group which, in turn, belongs to another group, only the first group is returned.

Configuring Advanced LDAP Settings

The Advanced LDAP settings configure the desired attribute/value when searching for a user record in an LDAP/Active Directory database. The feature is disabled by default, which means that no extra requirement is added when searching for a user record.

To configure the advanced settings, use the following commands

Table 42
Configuring Advanced LDAP Settings

/cfg/doamin #/aaa/auth #/ldap/adv followed by:	
enaxfilter true|false	Enables the extra search filter. • true - The search filter is enabled. Specify the desired attribute/value using the commands below. • false -The search filter is disabled. The default value is false.
xfilteratt	Sets the desired attribute when searching for user records. User records that contain this attribute and the value specified with the xfilterval command will be found. The default attribute is objectclass.
xfilterval	Sets the desired value when searching for user records. User records that contain the attribute specified with the xfilteratt command and this value will be found. The default value is person.

Configuring local database authentication

You can configure the Nortel SNAS domain to use local databases for portal (username/password) or MAC authentication. To configure the local database method, perform the following steps:

Step	Action
1	Create the Local database method (see "Adding the local database authentication method" (page 201)).
2	Populate the database (see "Managing the local portal database" (page 202)or "Managing the local MAC database" (page 206)).
3	Save a backup copy of the database (see "Managing the local portal database" (page 202) or "Managing the local MAC database" (page 206)).
4	Modify settings for the authentication method itself, if desired (see "Configuring authentication methods" (page 177)).

ATTENTION
If you ran the quick setup wizard during initial setup, Local database authentication has been created with authentication ID = 1. The local portal database contains one test user (`nha`), who belongs to a group called `nhauser`.

5 Set the authentication order (see "Specifying authentication fallback order" (page 209)).

--End--

Adding the local database authentication method

To create the Local database authentication method, use the following command:

`/cfg/doamin #/aaa/auth <auth ID>`

where **`auth ID`** is an integer in the range 1 to 63 that uniquely identifies the authentication method in the Nortel SNAS domain. If you do not specify the **`auth ID`** in the command, you are prompted for it.

When you first create the method for the domain, you must enter the authentication ID. After you have created the method and defined a name for it, you can use either the ID or the name to access the method for configuration.

The command to create the authentication ID launches a wizard. When prompted, enter the following information. You can later modify all settings for the specific local database configuration (see "Configuring authentication methods" (page 177) and "Managing the local portal database" (page 202)).

- authentication type—options are **`radius`** | **`ldap`** | **`local`**. Enter **`local`**.
- authentication method name (`auth name`)—a string that specifies a name for the method. After you have defined a name for the method, you can use either the method name or the **`auth ID`** to access the **Authentication** menu. In future releases of the Nortel SNAS software, you will be able to reference this string in a client filter, so that authentication to the database in question becomes a condition for access rights for a group.
- user name—a string that specifies a unique user login name. This item creates the first entry in the local database. To fully populate the database, add more users later (see "Managing the local portal database" (page 202)).
  There are no restrictions on the Nortel SNAS regarding acceptable user names. However, if you want the user name in the local database to mirror the Windows login name, observe Windows username conventions (for example, keep the length to no more than 32 characters).

- password (passwd)—the password that applies to the user you specified.
- group name—the name of the group to which the specified user belongs. The group must exist in the Nortel SNAS domain. To view available group names, press TAB.

ATTENTION
The prompt implies that you can enter multiple group names for a user, but the Nortel SNAS does not allow membership in multiple groups. If you enter multiple group names, the first group name entered is the one that will be returned to the Nortel SNAS after authentication.

The **Authentication** menu .

Figure 10 "Authentication menu commands—RADIUS" (page 182) shows sample output for the Local method for the **/cfg/doamin #/aaa/auth <auth ID>** command and commands on the **Authentication** menu.

Figure 12
Authentication menu commands—local database

```
>> Main# /cfg/domain 1/aaa/auth
Enter auth id: (1-63) 4
Creating Authentication 4
Select one of radius, ldap or local: local
Auth name: local4
Entering: Local database menu
Enter user name: <username>
Enter passwd: <password>
Enter group names (comma separated): <group>
Leaving: Local database menu

------------------------------------------------------------
[Authentication 4 Menu]
   type     - Set authentication mechanism
   name     - Set auth name
   display  - Set auth display name
   radius   - RADIUS settings menu
   adv      - Advanced settings menu
   del      - Remove Authentication

>> Authentication 4#
```

Managing the local portal database

The local portal database provides a respository for usernames and passwords.

You can add users to the database in two ways:

- manually, using the **/cfg/doamin #/aaa/auth #/local/add** command
- by importing a database, using the **/cfg/doamin #/aaa/auth #/local/ import** command

ATTENTION
The imported database overwrites existing entries in the local database.

You can use the local database for authorization only, after an external authentication server has authenticated the user. To do so, use an asterisk (*) for the user password in the local database. For information about configuring the Nortel SNAS to perform external database authentication in conjunction with local database authorization, see "Configuring advanced settings" (page 179).

To manage users and their passwords in the local database, use the following command:

/cfg/doamin #/aaa/auth #/local

The **Local database** menu appears.

The **Local database** menu includes the following options:

Table 43
Managing the local portal database

/cfg/doamin #/aaa/auth #/local **followed by:**	
add <user name> <password> <group>	Adds a user to the local authentication database. You are prompted for the following information: • **user name**—a string that specifies a unique user logon name. There are no restrictions on the NSNAS regarding acceptable user names. However, if you want the user name in the local database to mirror the Windows login name, observe Windows username conventions (for example, keep the length to no more than 32 characters). When the client attempts to log on to the Nortel SNAS domain and local database authentication is applied, the client is

Table 43
Managing the local portal database (cont'd.)

	prompted for the user name and password you define for the database. • **password**—the password that applies to the user you specified. To use the local database for authorization only, after an external authentication server has authenticated the user, enter an asterisk (*). • **group**—the name of the group to which the specified user belongs. The group must exist in the NSNAS domain. The group name is used for authorization. To view available group names, press TAB or use the **/cfg/doamin #/aaa/ cur group** command.
passwd <user name> <password>	Changes the specified user's password in the local database.
groups <user name> <desired group>	Changes the specified user's group membership in the local database.
radattr<add> <list> <del>	Configures the RADIUS attribute in the local database.
del <user name>	Deletes the specified user from the local database.
list	Lists all users added to the local database by user name, password (encrypted), and group membership. The command a maximum of 100 database entries at a time. If there are more than 100 entries in the database, you can limit the display by using a string of characters directly followed by an asterisk (*). For example, the command **list jo*** all entries with user names starting with `jo`.

Table 43
Managing the local portal database (cont'd.)

import <protocol> <server> <filename> <key>	Imports a database from the specified TFTP/FTP/SCP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the import protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server. • **filename** is the name of the database file on the server. • **key** is the password key for user password protection. For a database file whose passwords were protected with a key when the file was exported, the key you must provide is the same as the password key provided at the time of export. If the file is not protected with a key, enter any characters (a minimum of four) when prompted. • FTP user name and password, if applicable. The file you import must be in ASCII format. Each row entry consists of values for user name, password, and group, separated by a colon (for example, `username:password:group`) Passwords in the imported database can be clear-text or encrypted. Clear-text passwords will be encrypted after import. The imported database overwrites existing entries in the local database.

Table 43
Managing the local portal database (cont'd.)

export <protocol> <server> <filename> <key>	Exports the local database to the specified TFTP/FTP/SCP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the export protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server. • **filename** is the name of the destination database file on the server (for example, `db.txt`). • **key** is the password key for user password protection. If you are not protecting the file with a key, enter any characters (a minimum of four) when prompted. • FTP user name and password, if applicable. The file is exported in ASCII format. Each row entry consists of values for user name, password (encrypted), and group, separated by a colon. The following is an example of an exported user record with the password encrypted: john:$2$7á?yLs...ßìöonž±†:trusted where 2 indicates an encrypted password

Managing the local MAC database

The local MAC database provides a repository for MAC addresses. There is no design limit on the number of addresses the database can hold and up to 10,000 addresses has been verified.

You can add MAC addresses to the database in three ways:

- using the **/cfg/doamin #/aaa/auth #/macdb/add** command
- using the **/cfg/doamin #/aaa/auth #/macdb/import** command to import a file that has been properly formatted
- using the MAC Registration portal provided at login when a user belongs to a group with **macreg** set to **True** (**/cfg/doamin #/aaa/group #/macreg**)

To manage MAC addresses and associated parameters, use the following command:

/cfg/doamin #/aaa/auth #/macdb

The **MAC database** menu appears.

The **MAC database** menu includes the following options:

Table 44
Managing the local MAC database

/cfg/doamin #/aaa/auth #/macdb followed by:	
add	Adds a MAC address to the local database. You are prompted for the following information: • **MAC address**—MAC address of the host • **user name**—username of the host operator; optional • **device type <PC> <phone> <passive>** — **PC**: when the host is a computer — **phone**: when the host is a supported IP telephone — **passive**: when the device does not have an operator (for examples: a printer, a video camera); it is recommended that passive devices belong to their own, unique group • **IP type <dhcp> <static>** — **dhcp**: when the IP address of the host is provided by a DHCP server — **static**: when the IP address of the host is static • **switch IP address**—IP address of the network access device that serves the host; optional; recommended when device type is passive • **group name(s)**—The name(s) or ID number(s) of the NSNA group(s) of which the host is a member; a list of available groups is provided; if there is more than one group, separate with a colon • **comments**—any ASCII string, up to 80 characters; optional

Table 44
Managing the local MAC database (cont'd.)

	Enter **apply** when the **MAC database#** prompt . Duplicate and wildcard MAC addresses are not supported in NSNA release 1.6.1
del <MAC address>	Deletes the specified MAC address from the database.
list	Lists all entries in the MAC database.
show	Shows a particular MAC entry from the MAC database.
import <protocol> <server> <filename>	Imports a database from the specified TFTP/FTP/SCP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the import protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server. • **filename** is the name of the database file on the server. The file you import must be in ASCII format. Each line must have the form: MAC address;user name;IP type;device type;IP address;switch IP;switch unit;switch port;group(s);comments. Use a colon to separate group names. For example: 00:14:22:BB:12:8B;printer2;static;passive;192.168.2.23;;;; printers;Room 314 printer The imported database overwrites the existing database.
export <protocol> <server> <filename>	Exports the local database to the specified TFTP/FTP/SCP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the export protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server. • **filename** is the name of the destination database file on the server (for example, `db.txt`). The file is exported in ASCII format. Each line entry has the form: MAC address;user name;IP type;device type;IP address;switch IP;switch unit;switch port;group(s);comments. Multiple group names are separated by a colon.
clear	Clears the MAC database.

Adding MAC addresses using the MAC Registration interface The MAC Registration interface allows you to add or modify MAC addresses from your PC. You must be a member of a group for which **macreg** is set to **True** (**/cfg/doamin #/aaa/group #/macreg**).

To add or modify a MAC address, perform the following steps:

Step	Action
1	Log in to the network.
2	Click the **MAC Register** tab.

The MAC Registration interface .

3	Complete the form.
4	Click the **Register** button.

A confirmation message is returned indicating that the MAC address has been registered.

5	Click the **Done** button. Repeat to add or modify another MAC address.

--End--

Additions or modifications to the MAC database do not affect current sessions.

Specifying authentication fallback order

Authentication in the Nortel SNAS is performed by checking client credentials against available authentication databases until the first match is found. You specify the order in which the Nortel SNAS applies the methods configured for the Nortel SNAS domain.

Perform this step even if there is only one method defined on the Nortel SNAS.

ATTENTION
For best performance, set the authentication order so that the method that supports the biggest proportion of users is applied first. However, if you use the Nortel SNAS local database as one of the authentication methods, Nortel recommends that you set the Local method to be first in the authentication order. The Local method is performed extremely fast, regardless of the number of users in the database. Response times for the other methods depend on such factors as current network load, server performance, and number of users in the database.

To specify the authentication fallback order, use the following command:

```
/cfg/doamin #/aaa/authorder <auth ID>[,<auth ID>]
```

When prompted, enter the authentication method IDs in the order in which you want the methods applied. Use a comma to separate the entries.

To view the currently configured authentication methods and their corresponding authentication IDs, use the **/cfg/doamin #/aaa/cur** command.

For example: You have configured Local database authentication under auth ID 1, RADIUS authentication under auth ID 2, and LDAP authentication under auth ID 3. You want the Nortel SNAS to check the local database first, then send requests to the LDAP server, then to the RADIUS server. Figure 13 "Authentication order command" (page 210) shows the required command.

Figure 13
Authentication order command

```
>> Main# /cfg/domain 1/aaa/authorder
Current value: ""
Enter auth order (comma separated): 1,3,2

>> AAA# apply
Changes applied successfully.
```

Managing system users and groups

This chapter includes the following topics:

User rights and group membership

There are three groups of system users who routinely access the system for configuration and management:

- admin (administrator)
- certadmin (certificate administrator)
- oper (operator)

ATTENTION
There are two additional types of users with specialized functions: boot and root. For more information, see “Accessing the Nortel SNAS cluster” (page 381).

Group membership dictates user rights, as shown in Table 45 "Group membership and user rights" (page 212). When a user is a member of more than one group, user rights accumulate. The admin user, who by default is a member of all three groups, therefore has the same user rights as granted to members in the certadmin and oper group, in addition to the specific user rights granted by the admin group membership. The most permissive user rights become the effective user rights when a user is a member of more than one group. For more information about default user groups and related access levels, see “Accessing the Nortel SNAS cluster” (page 381).

Table 45
Group membership and user rights

Group Account	User account	Rights					
		System		Group		Password	
		Add user	Delete user	Add user	Delete user	Change own	Change others
admin	admin	Yes	Yes	Yes, to own gro up	Yes	Yes	Yes, if Admin is a member of the oth er user's first group
certadmin	admin	No	No	Yes, to own gro up	No	Yes	No
oper	oper admi n	No	No	Yes, to own gro up	No	Yes	No

Managing system users and groups

To manage system users and groups, access the **User** menu by using the following command:

```
/cfg/sys/user
```

From the **User** menu, you can configure and manage the following:

- add new users (for a detailed example, see "Adding a new user" (page 218))
- reassign users (for a detailed example, see "Changing a users group assignment" (page 221))
- change passwords (for a detailed example, see "Changing passwords" (page 223))
- delete users (for a detailed example, see "Deleting a user" (page 225))

For detailed information about the CLI commands, see "CLI configuration examples" (page 218).

Roadmap of system user management commands

The following roadmap lists all the CLI commands to configure and manage system users for the Nortel SNAS cluster. Use this list as a quick reference or click on any entry for more information:

Table 46
Roadmap of system user commands

Command	Parameter
`/cfg/sys/user`	`password <old password> <new password> <confirm new password>`
	`expire <time>`
	`list`
	`del <username>`
	`add <username>`
	`caphrase`
`/cfg/sys/user/edit <username>`	`password <own password> <user password> <confirm user password>`
	`cur`
`/cfg/sys/user/edit <username>/groups`	`list`
	`del <group index>`
	`add admin | oper | certadmin`

Managing user accounts and passwords

To change the password for the currently logged on user and to add or delete user accounts, access the **User** menu by using the following command:

```
/cfg/sys/user
```

The **User** menu appears.

The **User** menu includes the following options:

Table 47
Managing user accounts and passwords

`/cfg/sys/user` **followed by:**	
`password <old password> <new password> <confirm new password>`	Allows you to change your own password. Passwords can contain spaces and are case sensitive. The change takes effect as soon as you execute the command.

Table 47
Managing user accounts and passwords (cont'd.)

/cfg/sys/user **followed by:**	
expire <time>	Sets an expiration time for system user passwords. The time applies to all system users. The counter starts from when the password was last set. The first time the system user logs on after the specified time has expired, the user is prompted for a new password. • **time** is the length of time in days (d), hours (h), minutes (m), or seconds (s or unspecified). The default unit is seconds. The default expiration time is 0 seconds (no expiry). If the time you specify combines time units, the format is DDdHHhMMmSS. For example, to make all passwords expire in 30 days, 2 hours, and 45 minutes, enter **30d2h45m**..
list	Lists all user accounts. The three built-in users (admin, oper, and root) are always listed.
del <username>	Removes the specified user account from the system. Of the three built-in users (admin, oper, and root), only the oper user can be deleted. You must have administrator rights in order to delete user accounts. **ATTENTION** When you delete a user, the user's group assignment is also deleted. If you are deleting a user who is the sole member of a group, none of the remaining users on the system can then be added to that group. Existing users can only be added to a group by a user who is already a member of that group. Before deleting a user, verify that the user is not the sole member of a group.

Table 47
Managing user accounts and passwords (cont'd.)

/cfg/sys/user **followed by:**	
add <username>	Adds a user account to the system. The maximum length of the user name is 255 characters. No spaces are allowed. After adding a user account, you must also assign the user account to a group (see "Managing user groups" (page 217)). You must have administrator rights in order to add user accounts.
edit <username>	Accesses the **User <username>** menu, in order change user settings (see "Managing user settings" (page 216)). You must have administrator rights in order to change a user's settings. You must also be a member of the first group listed for the other user.
caphrase	Sets the certificate administrator's passphrase for encrypted private keys in a configuration backup, if the certificate administrator role has been separated from the administrator role. If the admin user is a member of the certadmin group (the default setting), the admin user is prompted for an export passphrase to protect the private keys in the configuration dump each time the **/cfg/ptcfg** command is used. Set a certificate administrator export passphrase only if the admin user has removed himself or herself from the certadmin group and added a certificate administrator user with certadmin group rights. When a configuration backup is performed using the **/cfg/ptcfg** command, the certadmin export passphrase is automatically used (without prompting the user) to protect the encrypted private keys. When the **/cfg/gtcfg** command is used to restore a configuration backup from a file exchange server, the user is prompted for the correct certadmin passphrase, as defined using the **caphrase** command.

Table 47
Managing user accounts and passwords (cont'd.)

/cfg/sys/user **followed by:**	
	ATTENTION The **caphrase** menu command is displayed only when the logged on user is a member of the certadmin group.

Managing user settings

You must have administrator rights in order to change a user's settings. You must also be a member of the other user's first group (the first group listed for the other user when you use the **/cfg/sys/user/edit <username> /groups/list** command).

To set or change the login password for a specified user and to view and manage group assignments, access the **User <username>** menu by using the following command:

/cfg/sys/user/edit <username>

The **User <username>** menu appears.

The **User <username>** menu includes the following options:

Table 48
Managing user settings

/cfg/sys/user/edit <username> **followed by:**	
password <own password> **<user password>** **<confirm user password>**	Sets the login password for the specified user. Passwords can contain spaces and are case sensitive.
groups	Accesses the **Groups** menu, in order to manage user group assignments (see "Managing user groups" (page 217)).
cur	the current group settings for the specified user.

Managing user groups

All users must belong to at least one group. Only an administrator user can add a new user account to the system, but any user can grant an existing user membership in a group to which the granting user belongs.

By default, the administrator user is a member of all three built-in groups (admin, oper, certadmin) and can therefore add a new user to any of these groups. However, a certificate administrator, who is a member of the certadmin group only, can add an existing user to the certadmin group only.

If a user belongs to only one group and you want to change the user's group membership, add the user to the new group first, and then remove the user from the old one.

If a user belongs to several groups, the first group, according to CLI numbering, determines the enforcement filters and VLANs that are applied.

To set or change a user's group assignment, access the **Groups** menu by using the following command:

`/cfg/sys/user/edit <username> /groups`

The **Groups** menu appears.

The **Groups** menu includes the following options:

Table 49
Managing user groups

`/cfg/sys/user/edit <username> /groups` **followed by:**	
`list`	Lists all groups to which the user is currently assigned, by group index number.
`del <group index>`	Removes the user from the specified group. • **`group index`** is an integer indicating the group index number You must have administrator rights in order to remove other users from groups.
`add admin|oper|certadmin`	Assigns the user to one of the built-in groups (admin, oper, certadmin).

CLI configuration examples

This section includes the following detailed examples:

Adding a new user

To add a new user to the system, you must be a member of the admin group. By default, only the admin user is a member of the admin group.

In this configuration example, a certificate administrator user is added to the system, and then assigned to the certadmin group. The certificate administrator specializes in managing certificates and private keys, without the possibility to change system parameters or configure virtual SSL servers. A user who is a member of the certadmin group can therefore access the Certificate menu (**/cfg/cert**), but not the SSL Server 1001 menu (**/cfg/domain #/server/ssl**). On the System menu (**/cfg/sys**), the certadmin user has access only to the User submenu (**/cfg/sys/user**).

Step	Action
1	Log on to the Nortel SNAS cluster as the **admin** user.

```
login: admin
Password: ( admin user password)
```

2 Access the User Menu.

```
>> Main# /cfg/sys/user

-------------------------------------------------
---------
[User Menu]
passwd - Change own password
list - List all users
del - Delete a user
add - Add a new user
edit - Edit a user
caphrase - Certadmin export passphrase
>> User#
```

3 Add the new user and designate a user name.

The maximum length for a user name is 255 characters. No spaces are allowed. Each time the new user logs in to the Nortel SNAS cluster, the user must enter the name you designate as the user name in this step.

```
>> User# add
Name of user to add: cert_admin (maximum 255 characters,
no spaces)
```

4 Assign the new user to a user group.

You can only assign a user to a group in which you yourself are a member. When this criterion is met, users can be assigned to one or more of the following three groups:

- oper
- admin
- certadmin

By default, the admin user is a member of all groups above, and can therefore assign a new or existing user to any of these groups. The group assignment of a user dictates the user rights and access levels to the system.

```
>> User# edit cert_admin
>> User cert_admin# groups/add
Enter group name: certadmin
```

5 Verify and apply the group assignment.

When you enter the **list** command, the current and pending group assignment of the user being edited is listed by index number and group name. Because the cert_admin user is a new user, the current group assignment listed by Old: is empty.

```
>> Groups# list
Old:
Pending:
  1:  certadmin
>> Groups# apply
Changes applied successfully.
```

6 Define a login password for the user.

When the user logs in to the Nortel SNAS cluster the first time, the user will be prompted for the password you define in this step. When successfully logged on, the user can change his or her own password. The login password is case sensitive and can contain spaces.

```
>> Groups# /cfg/sys/user
>> User# edit cert_admin
>> User cert_admin# password
Enter admin's current password: ( admin user password)
Enter new password for cert_admin: ( cert_admin user
password)
Re-enter to confirm: (reconfirm cert_admin user password)
```

7 Apply the changes.

```
>> User cert_admin# apply
Changes applied successfully.
```

8 Let the Certificate Administrator user define an export passphrase.

This step is only necessary if you want to fully separate the Certificate Administrator user role from the Administrator user role. If the admin user is removed from the certadmin group (as in Step 9), a Certificate Administrator export passphrase (caphrase) must be defined.

As long as the admin user is a member of the certadmin group (the default configuration), the admin user is prompted for an export passphrase each time a configuration backup that contains private keys is sent to a TFTP/FTP/SCP/SFTP server (command: **/cfg/ptcfg**). When the admin user is not a member of the certadmin group, the export passphrase defined by the Certificate Administrator is used instead to encrypt private keys in the configuration backup. The encryption of private keys using the export passphrase defined by the Certificate Administrator is performed transparently to the user, without prompting. When the configuration backup is restored, the Certificate Administrator must enter the correct export passphrase.

ATTENTION
If the export passphrase defined by the Certificate Administrator is lost, configuration backups made by the admin user while he or she was not a member of the certadmin group cannot be restored.

The export passphrase defined by the Certificate Administrator remains the same until changed by using the **/cfg/sys/user/caphrase** command. For users who are not members of the certadmin group, the **caphrase** command in the User menu is hidden. Only users who are members of the certadmin group should know the export passphrase. The export passphrase can contain spaces and is case sensitive.

```
>> User cert_admin# ../caphrase
Enter new passphrase:
Re-enter to confirm:
Passphrase changed.
```

9 Remove the admin user from the certadmin group.

Again, this step is only necessary if you want to fully separate the Certificate Administrator user role from the Administrator user role. Note however, that once the admin user is removed from the certadmin group, only a user who is already a member of the certadmin group can grant the admin user certadmin group membership anew.

When the admin user is removed from the certadmin group, only the Certificate Administrator user can access the Certificate menu (**/cfg/cert**).

```
>> User# edit admin
>> User admin# groups/list
 1:  admin
 2:  oper
 3:  certadmin
>> Groups# del 3
```

ATTENTION
It is critical that a Certificate Administrator user is created and assigned certadmin group membership before the admin user is removed from the certadmin group. Otherwise there is no way to assign certadmin group membership to a new user, or to restore certadmin group membership to the admin user, should it become necessary.

10 Verify and apply the changes.

```
>> Groups# list
Old:
 1:  admin
 2:  oper
 3:  certadmin
Pending:
 1:  admin
 2:  oper
>> Groups# apply
```

--End--

Changing a users group assignment

Only users who are members of the admin group can remove other users from a group. All users can add an existing user to a group, but only to a group in which the "granting" user is already a member. The admin user, who by default is a member of all three groups (admin, oper, and certadmin) can therefore add users to any of these groups.

Step	Action

1 Log on to the Nortel SNAS cluster.

In this example the cert_admin user, who is a member of the certadmin group, will add the admin user to the certadmin group. The example assumes that the admin user previously removed himself or herself from the certadmin group, in order to fully separate the Administrator user role from the Certificate Administrator user role.

```
login: cert_admin
Password: ( cert_admin user password)
```

2 Access the User Menu.

```
>> Main# /cfg/sys/user

-------------------------------------------------
---------
[User Menu]
passwd - Change own password
list - List all users
del - Delete a user
add - Add a new user
edit - Edit a user
caphrase - Certadmin export passphrase
>> User#
```

3 Assign the admin user certadmin user rights by adding the admin user to the certadmin group.

```
>> User# edit admin
>> User admin# groups/add
Enter group name: certadmin
```

ATTENTION
A user must be assigned to at least one group at any given time. If you want to replace a user's single group assignment, you must therefore always first add the user to the desired new group, then remove the user from the old group.

4 Verify and apply the changes.

```
>> Groups# list
Old:
 1:  admin
 2:  oper
Pending:
 1:  admin
 2:  oper
 3:  certadmin
>> Groups# apply
```

--End--

Changing passwords

Changing your own password All users can change their own password. Login passwords are case sensitive and can contain spaces.

Step	Action
1	Log on to the Nortel SNAS cluster by entering your user name and current password.

```
login: cert_admin
Password: ( cert_admin user password)
```

2 Access the User Menu.

```
>> Main# /cfg/sys/user

-----------------------------------------------------
---------
[User Menu]
passwd - Change own password
list - List all users
del - Delete a user
add - Add a new user
edit - Edit a user
caphrase - Certadmin export passphrase
>> User#
```

Type the **passwd** command to change your current password.

When your own password is changed, the change takes effect immediately without having to use the **apply** command.

```
>> User# passwd
Enter cert_admin's current password: (current cert_admin user password)
Enter new password: (new cert_admin user password)
Re-enter to confirm: (reconfirm new cert_admin user password)
Password changed.
```

--End--

Changing another users password Only the admin user can change another user's password, and then only if the admin user is a member of the other user's first group (the group that is listed first for the user with the **/cfg/sys/user/edit <username>/groups/list** command). Login passwords are case sensitive and can contain spaces.

Step	Action
1	Log on to the Nortel SNAS cluster as the admin user.

```
login: admin
Password: ( admin user password)
```

2 Access the User Menu.

```
>> Main# /cfg/sys/user

------------------------------------------------------
---------
[User Menu]
passwd - Change own password
list - List all users
del - Delete a user
add - Add a new user
edit - Edit a user
caphrase - Certadmin export passphrase
>> User#
```

3 Specify the user name of the user whose password you want to change.

```
>> User# edit
Name of user to edit: cert_admin
```

4 Type the **password** command to initialize the password change.

```
>> User cert_admin# password
Enter admin's current password: ( admin user password)
Enter new password for cert_admin: (new password for user being edited)
Re-enter to confirm: (confirm new password for user being edited)
```

5 Apply the changes.

```
>> User cert_admin# apply
Changes applied successfully.
```

--End--

Deleting a user

To delete a user from the system, you must be a member of the admin group. By default, only the admin user is a member of the admin group.

ATTENTION

Remember that when a user is deleted, that user's group assignment is also deleted. If you are deleting a user who is the sole member of a group, none of the remaining users on the system can then be added to that group. Existing users can only be added to a group by a user who is already a member of that group. Before deleting a user, you may therefore want to verify that the user is not the sole member of a group.

Step	Action

1 Log on to the Nortel SNAS cluster as the **admin** user.

```
login: admin
Password: ( admin user password)
```

2 Access the User Menu.

```
>> Main# /cfg/sys/user

-----------------------------------------------------
---------
[User Menu]
passwd - Change own password
list - List all users
del - Delete a user
add - Add a new user
edit - Edit a user
>> User#
```

3 Specify the user name of the user you want to remove from the system configuration.

In this example, the cert_admin user is removed from the system. To list all users currently added to the system configuration, use the **list** command.

```
>> User# del cert_admin
```

4 Verify and apply the changes.

The imminent removal of the cert_admin user is indicated as a pending configuration change by the minus sign (-). To cancel a configuration change that has not yet been applied, use the **revert** command.

```
>> User# list
  root
  admin
  oper
  -cert_admin
>>User# apply
```

--End--

Customizing the portal and user logon

This chapter includes the following topics:

Overview

The end user accesses the Nortel SNAS network through the Nortel SNAS portal. You can customize the end user experience by configuring the following logon and portal features:

- “Captive portal and Exclude List” (page 228)
  - “Exclude List” (page 228)
- “Portal display” (page 230)
  - “Portal look and feel” (page 230)
  - “Language localization” (page 233)
  - “Linksets and links” (page 234)

Captive portal and Exclude List

When the Nortel SNAS is configured to function as a captive portal, the Nortel SNAS acts as a DNS proxy while clients are in the Red VLAN. The captive web portal:

- accepts redirected HTTP/HTTPS requests from the clients
- resolves unknown names to a fixed IP address
- receives and manages communication requests from the clients to unauthorized network resources
- redirects client requests to an authentication page served by the portal

The DHCP server must be configured to assign the portal Virtual IP address (pVIP) as the DNS server when the client is in the Red VLAN.

The DHCP server is configured to specify the regular DNS servers for the scopes for the Green and Yellow VLANs. Once the client has been authenticated and is in a Green or Yellow VLAN, DNS requests are forwarded in the regular way to the corporate DNS servers.

For information about configuring the captive portal, see “Configuring the captive portal” (page 240).

Exclude List

The Exclude List is a configurable list of domain names that will not be captured by the Nortel SNAS. The DNS server in the captive portal forwards requests for domain names in the Exclude List directly to the corporate DNS servers.

In order to speed up client logon, add to the Exclude List any domain names for URLs that are routinely accessed during client logon or startup sequences. The Exclude List entry can be the full domain name or an expression.

By default, the captive portal Exclude List includes the following:

- windowsupdate
  This will match all automatic Windows update domain names used by browsers, for example:

— windowsupdate.com

— windowsupdate.microsoft.com

— download.windowsupdate.microsoft.com

For information about configuring the Exclude List, see “Configuring the Exclude List” (page 240).

Table 50 "Allowed regular expressions and escape sequences" (page 229) lists the regular expressions and escape sequences you can use in an Exclude List entry. The set of allowable regular expressions is a subset of the set found in egrep and in the AWK programming language. The escape sequences are allowed in Erlang strings.

Table 50
Allowed regular expressions and escape sequences

String	Usage
Expressions	
c	Matches the non-metacharacter *c*.
\c	Matches the literal character *c* (see escape sequence).
.	Matches any character.
^	Matches the beginning of a string.
$	Matches the end of a string.
[abc...]	Character class, which matches any of the characters *abc....* Character ranges are specified by a pair of characters separated by a hyphen (-).
[^abc...]	Negated character class, which matches any character except *abc....*
r1|r2	Alternation—matches either r1 or r2.
r1r2	Concatenation — matches r1 and then r2.
r+	Matches one or more *r* ’s.
r*	Matches zero or more *r* ’s.
r?	Matches zero or one *r* ’s.
(r)	Grouping—matches *r*.
Escape sequences	
\b	backspace
\f	form feed
\n	newline (line feed)

Table 50
Allowed regular expressions and escape sequences (cont'd.)

\r	carriage return
\t	tab
\e	escape
\v	vertical tab
\s	space
\d	delete
\ddd	the octal value *ddd*
\	literal character For example: \c for literal character *c*, \\ for backslash, \" for double quotation marks (")

Portal display

You can modify the following features of the portal display and behavior:

- portal look and feel (see "Portal look and feel" (page 230))
- language used (see "Language localization" (page 233))
- links (see "Linksets and links" (page 234))
- post-authentication behavior (see "Automatic redirection to internal sites" (page 236))

Portal look and feel

You can customize the colors, logos, icons, and text used on the portal page. You can also add custom content, such as Java applets, to the portal. You can then add links to the portal page to make the content available to clients.

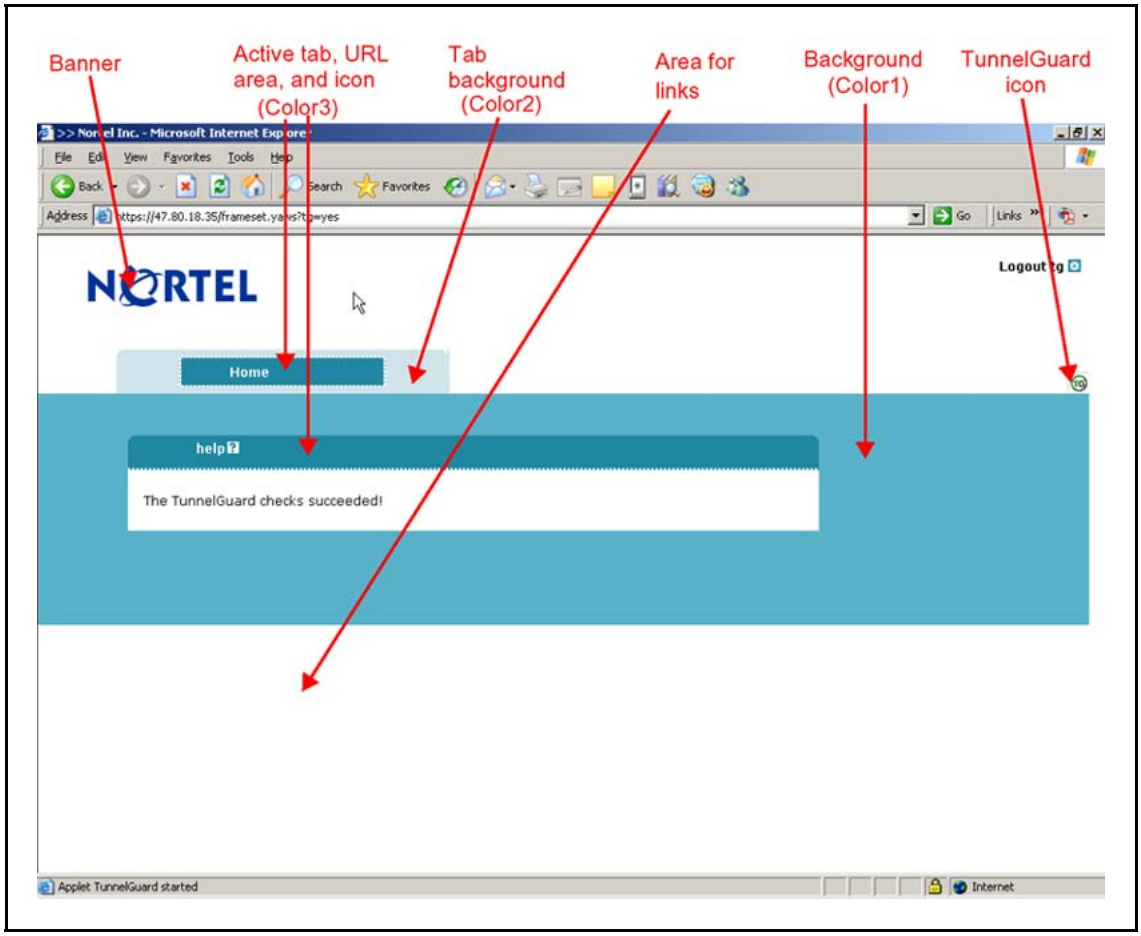
This section includes information about the following topics:

- "*Default appearance*" (page 230)
- "*Colors*" (page 231)

For information about the commands to configure the portal look and feel, see "Configuring the portal display" (page 244).

Default appearance Figure 14 "Default appearance of the portal Home tab" (page 231) shows the default portal Home tab.

Figure 14
Default appearance of the portal Home tab



Colors There are four colors used on the portal page:

- color1—the large background area below the tabs
- color2—the background area behind the tab labels
- color3—the fields, information area, and clean icons on the active tab
- color4—not used

There are five optional color themes. The themes are predefined sets of web-safe colors that complement each other.

- aqua
- apple
- jeans
- cinnamon
- candy

You can change the individual colors, but Nortel recommends using the color themes to change the look and feel of the portal page. If you change the portal colors, use colors that are considered web safe. Also consider how the applied colors fit with your company logo and brand.

The colors are specified using hexadecimal codes. Table 51 "Common colors, with hexadecimal codes" (page 232) lists the hexadecimal values for some commonly used web-safe colors. For additional color values, use an Internet search engine to find web sites offering comprehensive listings.

Table 51
Common colors, with hexadecimal codes

Color	Hexadecimal code
White	FFFFFF
Black	000000
Dark gray	A9A9A9
Light gray	D3D3D3
Red	FF0000
Green	008000
Blue	0000FF
Yellow	FFFF00
Orange	FFA500
Violet	EE82EE
Dark violet	9400D3
Pink	FFC0CB
Brown	A52A2A
Beige	F5F5DC
Lime green	32CD32
Light green	90EE90
Dark blue	00008B
Navy	000080
Light skyblue	87CEFA
Medium blue	0000CD
Dark red	8B0000

For the commands to configure the colors used on the portal, see “Changing the portal colors” (page 249).

For examples of how you can use macros to configure links and redirection to internal sites, see “Automatic redirection to internal sites” (page 236).

Self service portal

The Nortel SNAS self-service portal provides a web-based ‘help desk’ for users to collect information about their network connection, compliance, user status, and also for provisioning a guest access for users. This can be customized by using localized language files. The Nortel Health Agent runs on non-English versions of the operating systems.

Language localization The default English-language dictionary file contains entries for the text for tab names, general text, messages, buttons, and field labels on the portal page. The entries in the dictionary file can be translated into another language. You can then set the portal to display the translated text.

The languages supported by the Nortel SNAS are configured for the system, but the language selected for the portal is a domain parameter.

The Nortel SNAS uses ISO 639 language codes to track languages that have been added to the configuration. English (en) is the predefined language and is always present.

To change the language displayed for tab names, general text, messages, buttons, and field labels on the portal page, do the following:

Step	Action
1	Export the language definition template (see “Configuring language support” (page 242)).
2	Translate the language definition template file.

a Open the file with a text editor such as Notepad.

b Verify that the **`charset`** parameter specified in the Content-Type entry is set according to the character encoding scheme you are using. For example:

```
"Content-Type:  text/plain; charset=iso-8859-1/n"
```

c Translate the entries displayed under `msgstr` (message string).

ATTENTION
Do not translate the entries under `msgid` (message id).

There are useful Open Source software tools for translating po files. Search for *po files editor* in your web search engine to find tools that run on Windows and Unix. A translation tool is particularly useful when a new version of the Nortel SNAS software is released: you can export the new template file supplied with the software and merge it with a previously translated language file, so that only new and changed text strings need to be translated.

3 Import the translated language definition file (see "Configuring language support" (page 242)).

4 Set the portal to display the new language (see "Setting the portal display language" (page 243)).

--End--

Linksets and links

You can add the following types of links to the portal Home tab:

- External—links directly to a web page. Suitable for external web sites.
- FTP—links to a directory on an FTP server.

A linkset is a set of one or more links. Each linkset configured for the domain can be mapped to one or more groups and extended profiles in the domain. After the client has been authenticated, the client's portal page all the links included in the linksets associated with the client's group. The client's portal page also all the linksets associated with the client's extended profile. For information about mapping linksets to groups and extended profiles, see "Mapping linksets to a group or profile" (page 167).

Autorun linksets You can enable an autorun feature for a linkset so that all links defined for that linkset execute automatically after the client has been authenticated. For example, you can configure an autorun linkset to automatically link to the URL of the remediation server, and then map this linkset to all extended profiles which filter for clients who fail the Nortel Health Agent host integrity check.

No links for the autorun linkset display on the portal page. Each link in the linkset opens in a new browser window. If the autorun linkset includes multiple links, multiple browser windows will open. For information about configuring autorun, see "Configuring linksets" (page 251).

The linkset autorun feature is similar to the portal feature allowing automatic redirection to internal sites (see "Automatic redirection to internal sites" (page 236)). The linkset feature allows more granular control of this functionality. Also, unlike the linkset autorun feature, the automatic redirection feature does not open the link in a new browser window.

Planning the linksets Plan your configuration so that linksets containing common links are separate from linksets containing group-specific links. Also ensure that the links you are providing to resources do not contradict the client's access rights.

You can control the order in which links display on the portal Home tab. Consider the following in your planning:

- Linksets for the group display after the linksets for the client's extended profile.
- The index number you assign to the linkset controls the order in which the linksets display. You assign the index number when you map the linkset to the group or extended profile (see "Mapping linksets to a group or profile" (page 167)).
- The index number you assign to the link controls the order in which the links display within the linkset. You assign the index number when you include the link in the linkset (see "Configuring links" (page 253)).

Macros

Macros are inline functions you can use to insert variable arguments in text, in order to customize the portal for individual users.

The following macros are available for use as arguments in parameters for links, display text, and redirection commands:

- **<var:portal>**—expands to the domain name of the portal
- **<var:user>**—expands to the user name of the currently logged in client
- **<var:password>**—expands to the password of the currently logged in client
- **<var:group>**—expands to the name of the group of which the currently logged in client is a member

Automatic redirection to internal sites

You can configure the portal to automatically redirect authenticated clients to an internal site. Unlike the linkset autorun feature, automatic redirection does not open a new browser window. Rather, it replaces the default Home page in the internal frame on the portal browser page. As long as the browser remains open, the session remains logged in.

The commands to configure automatic redirection require you to specify the URL to which the clients will be redirected, prefixed by the portal address (see “Configuring the portal display” (page 244)).

Examples of redirection URLs and links

Table 52 "Examples of redirection URLs and link text" (page 236) shows example specifications for redirection URLs and associated links. In these examples:

- the portal address is nsnas.example.com
- the address to which you want to redirect clients is inside.example.com

Table 52
Examples of redirection URLs and link text

Purpose	Redirection URL or link text
Redirect the client to an internal site.	Redirection URL: https://nsnas.example.com/http/inside.example.com or https://<var:portal>/http/inside.example.com
Redirect the client to a password-protected site. **ATTENTION** The user name and password on the intranet site and the portal must be identical.	Redirection URL: https://<var:portal>/http/<var:user>:<var:password>@inside.example.com/protected

Table 52
Examples of redirection URLs and link text (cont'd.)

Purpose	Redirection URL or link text
Redirect clients to different sites, depending on their group membership (deptA or deptB).	Linktext (static text) entry: `<script>if ("<var:group>" == "deptA") { location.replace ("https://nsnas.example.com/http/inside.example.com/deptA.html");} else if ("<var:group>" == "deptB") { location.replace ("https://nsnas.example.com/http/inside.example.com/deptB.html");} </script>`
Insert a link on the internal site for the client to log off from the portal.	Link: `<a href=https://nsnas.example.com/logout.yaws> Logout from portal </a>`

Managing the end user experience

Nortel recommends that you consider the following ways in which you can manage the end user's experience:

- "Automatic JRE upload" (page 237)
- "Windows domain logon script" (page 238)

Automatic JRE upload

The Nortel SNAS portal requires the client device to be running a minimum version of the Java Runtime Environment (JRE) in order for the Nortel Health Agent applet to load properly. Nortel recommends adding the required JRE version and plugins.html as custom content to the portal. In this way, if the client does not meet the Java requirement and Nortel Health Agent does not load, the client will be presented with a logon screen to automatically download and install the required JRE.

To configure the portal to automate the process of updating the client's JRE version, perform the following steps:

Step	Action
1	Create the plugins.html file, with a link to the JRE installer that you want.
2	Download the JRE installer from the Sun Microsystems Java web site (http://www.java.com).

3 Bundle plugins.html and the JRE installer in a zip file.

4 Add the zip file as custom content to the portal.

--End--

For general information about adding custom content to the portal, see "Configuring custom content" (page 250). For information about the minimum JRE requirements, see *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.6.1 (NN47230-400)*, .

Windows domain logon script

Configure a Windows domain logon script to automatically launch the end user's browser and present the Nortel SNAS portal page on start-up. The exact requirements for the script depend on your particular network setup and usual modes of end-user access.

For an example of a very simple script and instructions on assigning the script to all users in the domain, see "Using a Windows domain logon script to launch the Nortel SNAS portal" (page 501).

Customizing the portal and logon

The following section describes the CLI commands to customize the portal and user logon.

Roadmap of portal and logon configuration commands

The following roadmap lists all the CLI commands to customize the portal and user logon. Use this list as a quick reference or click on any entry for more information.

Command	Parameter
`/cfg/doamin #/dnscapt`	`ena`
	`dis`
`/cfg/doamin #/dnscapt/exclude`	`list`
	`del <index name>`
	`add <domain name>`
	`insert <index number> <domain name>`
	`move <index number> <new index number>`
`/cfg/lang`	`import <protocol> <server> <filename> <code>`
	`export <protocol> <server> <filename>`
	`list`
	`vlist [<letter>]`

Command	Parameter
	del <code>
/cfg/doamin #/portal/lang	setlang <code>
	charset
	list
/cfg/doamin #/portal	import <protocol> <server> <filename>
	restore
	banner
	redirect <URL>
	logintext <text>
	iconmode clean | fancy
	linktext <text>
	linkurl on | off
	linkcols <columns>
	linkwidth <width>
	companynam
	ieclear on | off
/cfg/doamin #/portal/colors	color1 <code>
	color2 <code>
	color3 <code>
	color4 <code>
	theme default | aqua | apple | jeans | cinnamon | candy
/cfg/doamin #/portal/content	import <protocol> <server> <filename>
	export <protocol> <server> <filename>
	delete
	available
	ena
	dis
/cfg/doamin #/linkset <linkset ID>	name <name>
	text <text>
	autorun true | false
	del
/cfg/doamin #/linkset <linkset ID>/link <index>	move <new index>
	text <text>

Command	Parameter
	`type external | ftp`
	`del`
`/cfg/doamin #/linkset <linkset ID>/link <index>/external/quick`	
`/cfg/doamin #/linkset <linkset ID>/link <index>/ftp/quick`	

Configuring the captive portal

By default, the Nortel SNAS is set up to function as a captive portal. (For more information about the captive portal in the Nortel SNAS domain, see "Captive portal and Exclude List" (page 228).)

To configure the Nortel SNAS portal as a captive portal, use the following command:

```
/cfg/doamin #/dnscapt
```

The **DNS Capture** menu appears.

The **DNS Capture** menu includes the following options:

`/cfg/doamin #/dnscapt` **followed by:**	
`exclude`	Accesses the **DNS Exclude** menu, in order to configure the Exclude List (see "Configuring the Exclude List" (page 240)).
`ena`	Enables captive portal functionality.
`dis`	Disables captive portal functionality.

Configuring the Exclude List

The Exclude List is a list of domain names that will not be captured by the Nortel SNAS. (For more information about the Exclude List, see "Exclude List" (page 228).)

To create and manage the Exclude List, use the following command:

```
/cfg/doamin #/dnscapt/exclude
```

The **DNS Exclude** menu appears.

The **DNS Exclude** menu includes the following options:

/cfg/doamin #/dnscapt/exclude **followed by:**	
list	Lists the currently configured Exclude List entries by index number
del <index name>	Removes the Exclude List entry represented by the specified index number. The index numbers of the remaining entries adjust accordingly.
add <domain name>	Adds an entry to the Exclude List. • **domain name** is a string identifying the domain names to be forwarded directly to the corporate DNS servers For information about allowable expressions and escape sequences, see "Exclude List" (page 228). The Nortel SNAS assigns the next available index number to the entry.
insert <index number> <domain name>	Inserts an entry at a particular position in the list. The index number you specify must be in use. The index numbers of existing entries with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves an entry up or down the list. The index numbers of the remaining entries adjust accordingly.

Changing the portal language

To change the language displayed for tab names, general text, messages, buttons, and field labels on the portal page, do the following:

Step	Action
1	Export the language definition template (see "Configuring language support" (page 242)).
2	Translate the language definition template file (see "Language localization" (page 233)).
3	Import the translated language definition file (see "Configuring language support" (page 242)).

4 Set the portal to display the new language (see “Setting the portal display language” (page 243)).

--End--

Configuring language support

To manage the language definition files in the system, use the following command:

`/cfg/lang`

The **Language Support** menu appears.

The **Language Support** menu includes the following options:

`/cfg/lang` **followed by:**	
`import <protocol> <server> <filename> <code>`	Imports a ready-to-use language definition file from the specified TFTP/FTP/SCP/SFTP file exchange server. • **`protocol`** is the import protocol. Options are **`tftp`**|**`ftp`**|**`scp`**|**`sftp`**. • **`server`** is the host name or IP address of the server • **`filename`** is the name of the language definition file on the server • **`code`** is the ISO 639 language code to identify the language When you import the file, you are prompted to specify the ISO 639 language code. The language code is saved to the configuration together with the imported language definition file. To view valid language codes, use the **`/cfg/lang/vlist`** command. For more information about language support on the portal, see “Language localization” (page 233) .

/cfg/lang **followed by:**	
export <protocol> <server> <filename>	Exports the language definition template to the specified TFTP/FTP/SCP/SFTP file exchange server. • **protocol** is the export protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server • **filename** is the name of the language definition file • **code** is the ISO 639 language code to identify the language Once the template file has been exported and downloaded, you can translate screen text, such as button and field labels, directly in the file. Then upload the translated file to a TFTP/FTP/SCP/SFTP file exchange server and import it using the **/cfg/lang/import** command.
list	Lists the languages that have been added to the configuration, by language code and description. English (en) is the predefined language and is always present.
vlist [<letter>]	Lists all valid language codes and their corresponding description. To list all valid language codes beginning with a specific letter, specify the letter in the command.
del <code>	Deletes the language definition file for the specified language code. You cannot delete a language file that is currently in use. English (en) is the predefined language and cannot be deleted.

Setting the portal display language

To set the preferred language for the portal display, use the following command:

/cfg/doamin #/portal/lang

The **Portal Language** menu appears.

The **Portal Language** menu includes the following options:

/cfg/doamin #/portal/lang followed by:	
setlang <code>	Specifies the language to be used for the portal display. • code is the ISO 639 language code to identify the language Before you can set the preferred language, you must import the corresponding language definition file (see "Configuring language support" (page 242)). To view supported language codes, use the /cfg/doamin #/portal/lang/list command.
charset	Prints the character set that is currently in use on the portal.
list	Lists the currently supported languages, by language code and description.

Configuring the portal display

To modify the look and feel of the portal page that in the client's web browser, use the following command:

```
/cfg/doamin #/portal
```

The **Portal** menu appears.

The **Portal** menu includes the following options:

/cfg/doamin #/portal followed by:	
import <protocol> <server> <filename>	Imports a graphics file for the banner (in GIF format) from the specified TFTP/FTP/SCP/SFTP file exchange server. • protocol is the import protocol. Options are tftp | ftp | scp | sftp. • server is the host name or IP address of the server • filename is the name of the graphics file (.gif)

/cfg/doamin #/portal **followed by:**	
	When the download is complete and you apply the changes, the new image replaces the existing banner image on the portal web page. Clients who are currently logged on will not notice the change unless they reload the portal web page. The maximum size of the banner image file is 16 MB. If there are several Nortel SNAS domains, the total size of all imported banner image files must not exceed 16 MB. For more information about the customizable elements on the portal web page, see “Portal look and feel” (page 230).
restore	Restores the default Nortel banner.
banner	the file name of the banner image file currently in use.
redirect <URL>	Sets the URL to which clients are automatically redirected after authentication by the portal. • **URL** is the URL to which to direct the client, prefixed by the portal address For example, if the portal address is nsnas.example.com and you want to redirect clients automatically to inside.example.com, the URL parameter is: *https://nsnas.example.com/http/inside.example.com* Alternatively, you can use the <var:portal> macro to represent the portal address. With redirection configured, the client will not be able to access tabs on the portal page.

/cfg/doamin #/portal **followed by:**	
	To remove redirection, replace the previously specified URL with an empty string by pressing **Enter** at the URL prompt. For more information about using macros in URLs, see “Macros” (page 235). For more information about redirecting clients to internal sites, see “Automatic redirection to internal sites” (page 236).
logintext <text>	Specifies custom text to be displayed on the portal logon page. • **text** is an ordinary text string or HTML code You can type in the text or paste it in at the prompt. To signal the end of the string, press **Enter** to create a new line, type an ellipsis (...), and then press **Enter** again.
iconmode clean | fancy	Specifies the mode for the icons representing portal links (for example, file server links). • **clean** simple icons using a single color (color3) • **fancy** multicolored, shaded, and animated icons The default value is **fancy**. For more information about linksets and links, see “Linksets and links” (page 234). For information about configuring links, see “Configuring links” (page 253). For information about customizing the colors used on the portal page, see “Changing the portal colors” (page 249).

/cfg/doamin #/portal **followed by:**	
linktext <text>	Specifies static text to be displayed above the group links on the portal Home tab. The static text for all clients, but the links themselves may change, depending on the client's group membership. • **text** is an ordinary text string or HTML code You can type in the text or paste it in at the prompt. To signal the end of the string, press **Enter** to create a new line, type an ellipsis (...), and then press **Enter** again. You can use the **<var:user>** and **<var:group>** macros in the link text. For an example of using the <var:group> macro in a Java script linktext entry in order to configure group-controlled redirection to internal sites, see Table 52 "Examples of redirection URLs and link text" (page 236). For more information about using macros in links, see "Macros" (page 235). For more information about configuring links, see "Configuring links" (page 253).
linkurl on|off	Sets the display mode for the Enter URL field on the portal Home tab. Display mode options are: • **on**—the Enter URL field is displayed • **off**—the Enter URL field is not displayed The default is **on**.
linkcols <columns>	Sets the number of columns for the link table on the portal Home tab. • **columns** is a positive integer The default value is 2.

/cfg/doamin #/portal **followed by:**	
linkwidth <width>	Sets the width of the link table on the portal Home tab. The link table is adjusted to the left on the white area of the Home tab. The options for the table width are: • **auto**—the columns are distributed evenly across the Home tab • **<percent>**—specifies the percentage of the white area that will be used for the link table. The range is 1–100%. The default value is 100% (the entire white area will be used).
companynam	Specifies the company name to display on the portal page. The default is **Nortel**.
colors	Accesses the **Portal Colors** menu, in order to customize the color theme and individual colors used on the portal page (see "Changing the portal colors" (page 249)).
content	Accesses the **Portal Custom Content** menu, in order to provide custom content for the portal page (see "Configuring custom content" (page 250)).
lang	Accesses the **Portal Language** menu, in order to set the preferred language for the portal display (see "Setting the portal display language" (page 243)).
ieclear on|off	Controls use of the ClearAuthenticationCache feature available in Internet Explorer 6, SP 1 and later (IE). The feature is used to clear sensitive information (such as passwords and cookies) from the cache when a user logs out from a secure session. • **on**—the cache is cleared for all instances of the current process when the user logs off from the portal. The user will also be logged off from any other sites at the same time. • **off**—when the user logs off from the portal, the cache is not cleared until the user closes the browser

/cfg/doamin #/portal **followed by:**	
	The default value is **on**.

Changing the portal colors

To customize the colors used for the portal display, use the following command:

/cfg/doamin #/portal/colors

The **Portal Colors** menu appears.

The **Portal Colors** menu includes the following options:

/cfg/doamin #/portal/colors **followed by:**	
color1 <code>	Specifies the color for the large background area below the tabs. • **code** is the hexadecimal value for the color, including the # symbol (not case sensitive) The default value is #ACCDD5.
color2 <code>	Specifies the color for the background area behind the labels. • **code** is the hexadecimal value for the color, including the # symbol (not case sensitive) The default value is #D0E4E9.
color3 <code>	Specifies the color for the fields, information area, and clean icons on the active tab. • **code** is the hexadecimal value for the color, including the # symbol (not case sensitive) The default value is #2088A2.

/cfg/doamin #/portal/colors **followed by:**	
color4 <code>	Specifies the color fornon-active tabs. • **code** is the hexadecimal value for the color, including the # symbol (not case sensitive) The default value is #58B2C9.
theme default | aqua | apple | jeans | cinnamon | candy	Specifies the color theme for the portal. The default is **default**.

For more information about the portal colors and themes, see "*Colors*" (page 231) .

Configuring custom content

To add custom content, such as Java applets, to the portal, use the following command:

/cfg/doamin #/portal/content

The **Portal Custom Content** menu appears.

The **Portal Custom Content** menu includes the following options:

/cfg/doamin #/portal/content **followed by:**	
import <protocol> <server> <filename>	Imports a content file (in ZIP format) from the specified TFTP/FTP/SCP/SFTP file exchange server. • **protocol** is the import protocol. Options are **tftp | ftp | scp | sftp**.The default is **tftp**. • **server** is the host name or IP address of the server • **filename** is the name of the content file (.zip) on the server The file is saved in the portal's root directory and is automatically unpacked.

/cfg/doamin #/portal/content **followed by:**	
export <protocol> <server> <filename>	Exports a content file (in ZIP format) from the portal to the specified TFTP/FTP/SCP/SFTP file exchange server. • **protocol** is the export protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server • **filename** is the name of the content file (.zip)
delete	Deletes all uploaded content from the portal.
available	Shows remaining memory space available for custom content, in kilobytes (KB).
ena	Enables client access to custom content. The default is disabled.
dis	Disables client access to custom content.

Configuring linksets

A linkset is a set of links that display on the portal Home tab. For more information about linksets and links, see "Linksets and links" (page 234).

To create and configure a linkset, use the following command:

/cfg/doamin #/linkset <linkset ID>

where

linkset ID is an integer in the range 1 to 1024 that uniquely identifies the linkset in the Nortel SNAS domain.

ATTENTION
If you ran the quick setup wizard during initial setup, two linksets have been created: **nha_passed** (linkset ID = 1) and **nha_failed** (linkset ID = 2). The linksets are empty.

When you first create the linkset, if you do not specify the ID in the command, you will be prompted to enter the linkset ID or name. You must enter the ID for the new linkset. You will then be prompted to enter the linkset name. After you have created the linkset, you can use either the ID or the name to access the linkset for configuration.

The **Linkset** menu appears.

The **Linkset** menu includes the following options:

/cfg/doamin #/linkset <linkset ID> **followed by:**	
name <name>	Names or renames the linkset. After you have defined a name for the linkset, you can use either the linkset name or the linkset ID to access the **Linkset** menu. • **name** is a string that must be unique in the domain. The maximum length of the string is 255 characters. You reference the linkset name when mapping the linkset to groups or extended profiles using the **/cfg/doamin #/aaa/group #[/extend #]/linkset** command (see "Mapping linksets to a group or profile" (page 167)). When you map the linkset to a group, members of the group get access to all the links contained in the linkset. The links display on the portal Home tab.
text <text>	Specifies text to display as a heading above the linkset links on the portal Home tab. • **text** is an ordinary text string or HTML code The heading text is optional.

/cfg/doamin #/linkset <linkset ID> **followed by:**	
autorun true | false	Specifies whether autorun support is enabled or disabled. The options are: • **true**—autorun is enabled • **false**—autorun is disabled If enabled, all links defined for the linkset execute automatically after the client has been authenticated. No links for this linkset display on the portal Home tab. The default is disabled. For more information about the type of links you can configure, see "Linksets and links" (page 234).
link <index>	Accesses the **Link** menu, in order to create or configure links for the linkset (see "Configuring links" (page 253)). To view existing linksets, press **TAB** following the **link** command.
del	Removes the linkset from the current configuration.

Configuring links

To create and configure the links included in the linkset, use the following command:

/cfg/doamin #/linkset <linkset ID> /link <index>

where

index is an integer in the range 1 to 256 that indicates the position of the link in the linkset.

When you first create the link, if you do not specify the index in the command, you will be prompted to enter the index or name. You must enter the index for the new link. You will then be prompted to enter the following parameters:

- link text—a string that on the portal Home tab as the clickable link text. You can later modify the text by using the **text** command on the **Link** menu.
- type—the link type (**external** or **ftp**). The default is **external**. After you enter the link type, you automatically enter a wizard to configure type-specific settings for the link. You can later relaunch the wizard to modify the settings. For more information about the settings, see "Configuring external link settings" (page 255).

The **Link** menu appears.

The **Link** menu includes the following options:

/cfg/doamin #/linkset <linkset ID> /link <index> **followed by:**	
move <new index>	Moves the link to a new position in the linkset. The index numbers of existing link entries with this index number and higher are incremented by 1. • **new index** is an integer in the range 1 to 256 that indicates the position of the link in the linkset For example: You have two portal links, Link 1 and Link 2. To move Link 2 so it before Link 1 on the portal page, enter the following command: `>> Link 3# move 1` Link 2 becomes Link 1, and Link 1 becomes Link 2.
text <text>	Specifies text to display as the clickable link text on the portal Home tab. • **text** is an ordinary text string or HTML code Provide descriptive text that clearly identifies the targeted resource. The client sees only the link text, not the URL contained in the link.

/cfg/doamin #/linkset <linkset ID> /link <index> **followed by:**	
type external | ftp	Specifies the type of link. The options are: • **external**—directs the client to a web page. The external link is not secured by the Nortel SNAS. • **ftp**—directs the client to a directory on an FTP file exchange server The default is **external**. The **Link** menu changes to include a command corresponding to the specified link type. **ATTENTION** Nortel Secure Network Access Switch Software Release 1.6.1supports **external** links only.
external	Accesses the **External Settings** menu, in order to configure settings for the link (see "Configuring external link settings" (page 255)). This command only if the link type is **external**.
ftp	Accesses the **FTP Settings** menu, in order to configure settings for the link. This command only if the link type is **ftp**.
del	Removes the link from the current configuration.

Configuring external link settings

To launch the wizard to configure settings for a link to an external web page, use the following command:

/cfg/doamin #/linkset <linkset ID> /link <index> /external/quick

The wizard prompts you to enter the following settings:

- method—HTTP or HTTPS
- host—the host name or IP address of the web server
- path—the path on the web server. You must specify a path. A single slash (/) indicates the web server document root.

Configuring system settings

This chapter includes the following topics:

System settings apply to a cluster as a whole.

You can log on to either the Management IP address (MIP) or a Nortel SNAS host Real IP address (RIP) in order to configure the system.

Configuring the cluster

To configure the cluster, access the **System** menu by using the following command:

`/cfg/sys`

From the **System** menu, you can configure and manage the following:

- Management IP address (MIP) (see “Configuring system settings” (page 262))
- the Nortel SNAS host, including interfaces and ports (see “Configuring the Nortel SNAS host” (page 264))
- static routes (see “Configuring static routes” (page 270))
- date and time (see “Configuring date and time settings” (page 274))
- DNS settings (see “Configuring DNS servers and settings” (page 276))
- RSA servers (see “Configuring RSA servers” (page 279)) (not supported in Nortel Secure Network Access Switch Software Release 1.6.1)
- Syslog servers (see “Configuring syslog servers” (page 279))
- Access Lists (see “Configuring the Access List” (page 273))
- administrative applications, including
  - managing access for Telnet, SSH, and SONMP (see “Configuring administrative settings” (page 281))
  - configuring system management using SNMP (see “Configuring SNMP” (page 323))
  - enabling SRS administration (see “Enabling TunnelGuard SRS administration” (page 284))
  - managing Nortel SNAS host SSH keys (see “Configuring Nortel SNAS host SSH keys” (page 284))
  - managing RADIUS auditing (see “Configuring RADIUS auditing” (page 286))
  - managing RADIUS authentication of system users (see “Configuring authentication of system users” (page 290))
- user access (see “Managing system users and groups” (page 211))
- disabling SSL traffic trace commands (see “Configuring system settings” (page 262))

Roadmap of system commands

The following roadmap lists the CLI commands to configure cluster-wide parameters and the Nortel SNAS host within the cluster. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
/cfg/sys	mip <IPaddr>
	distrace
/cfg/sys/host <host ID>	ip <IPaddr>
	sysName <name>
	sysLocatio <location>
	license <key>
	gateway <IPaddr>
	ports
	hwplatform
	halt
	reboot
	delete
/cfg/sys/host <host ID>/interface <interface ID>	ip <IPaddr>
	netmask <mask>
	gateway <IPaddr>
	vlanid <tag>
	mode failover | trunking
	primary <port>
	delete
/cfg/sys/routes	list
	del <index number>
	add <IPaddr> <mask> <gateway>
/cfg/sys/host <host ID>/routes	list
	del <index number>
	add <IPaddr> <mask> <gateway>
/cfg/sys/host #/interface <interface ID>/routes	list
	del <index number>
	add <IPaddr> <mask> <gateway>
/cfg/sys/host #/port <port>	autoneg on|off
	speed <speed>
	mode full | half
/cfg/sys/host #/interface <interface ID>/ports	list
	del <port>

Command	Parameter
	add <port>
/cfg/sys/accesslist	list
	del <index number>
	add <IPaddr> <mask>
/cfg/sys/time	date <date>
	time <time>
	tzone
/cfg/sys/time/ntp	list
	del <index number>
	add <IPaddr>
/cfg/sys/dns	cachesize <entries>
	retransmit <interval>
	count <count>
	ttl <ttl>
	health <interval>
	hdown <count>
	hup <count>
/cfg/sys/dns/servers	list
	del <index number>
	add <IPaddr>
	insert <index number> <IPaddr>
	move <index number> <new index number>
/cfg/sys/rsa	rsaname <name>
	import <protocol> <server> <filename> [<FTP user name> <FTP password>]
	rmnodesecr
	del
/cfg/sys/syslog	list
	del <index number>
	add <IPaddr> <facility>
	insert <index number> <IPaddr> <facility>
	move <index number> <new index number>

Command	Parameter
/cfg/sys/adm	sonmp on | off
	clitimeout <interval>
	telnet on | off
	ssh on | off
	redist yes | no
/cfg/sys/adm/srsadmin	port <port>
	ena
	dis
/cfg/sys/adm/sshkeys	generate
	show
/cfg/sys/adm/sshkeys/knownhosts	list
	del <index number>
	add
	import <IPaddr>
/cfg/sys/adm/audit	vendorid
	vendortype
	ena
	dis
/cfg/sys/adm/audit/servers	list
	del <index number>
	add <IPaddr> <port> <shared secret>
	insert <index number> <IPaddr>
	move <index number> <new index number>
/cfg/sys/adm/auth	timeout <interval>
	fallback on | off
	ena
	dis
/cfg/sys/adm/auth/servers	list
	del <index number>
	add <IPaddr> <port> <shared secret>
	insert <index number> <IPaddr>
	move <index number> <new index number>
/cfg/sys/adm/abl	user_atmpt

Command	Parameter
	host_atmpt
	user_purge
	host_purge
	show
	clear
	ena
	dis
/cfg/sys/adm/abl/users	list
	del <index number>
	add <user name>
/cfg/sys/adm/abl/hosts	list
	del <index number>
	add <Host IP address>
/cfg/sys/adm/abl/hardenpass	length <Minimum length>
	lowercase <Lower case>
	uppercase <Upper case>
	digits <Digits>
	others <other characters>
	retry <maximum retries>
	ena
	dis

Configuring system settings

To view and configure cluster-wide system settings, use the following command:

```
/cfg/sys
```

The **System** menu appears.

The **System** menu includes the following options:

/cfg/sys **followed by:**	
mip <IPaddr>	Sets the MIP for the cluster. The MIP identifies the cluster and must be unique on the network. For more information, see "About the IP addresses" (page 42). **ATTENTION** Nortel does not recommend reconfiguring this parameter if you are logged on to the MIP, because you may lose connectivity. To reset the MIP, log on to the RIP instead.
host <host ID>	Accesses the **Cluster Host** menu, in order to configure a specific Nortel SNAS host (see "Configuring the Nortel SNAS host" (page 264)).
routes	Accesses the **Routes** menu, in order to manage static routes for the cluster when there is more than one interface (see "Configuring static routes" (page 270)).
time	Accesses the **Date and Time** menu, in order to configure date and time settings and to access Network Time Protocol (NTP) servers (see "Configuring date and time settings" (page 274)).
dns	Accesses the **DNS Settings** menu, in order to manage DNS servers and tune DNS settings (see "Configuring DNS servers and settings" (page 276)).
rsa <server ID>	Accesses the **RSA Servers** menu, in order to configure the RSA server (see "Configuring RSA servers" (page 279)). **ATTENTION** Not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
syslog	Accesses the **Syslog Servers** menu, in order to configure the Syslog servers for receiving log messages (see "Configuring syslog servers" (page 279)).
accesslist	Accesses the **Access List** menu, in order to control Telnet and SSH access to Nortel SNAS devices (see "Configuring the Access List" (page 273)).

/cfg/sys **followed by:**	
adm	Accesses the **Administrative Applications** menu, in order to set the CLI timeout value; manage Telnet, SSH, SNMP, and SONMP access to Nortel SNAS devices; enable SRS administration; generate SSH host keys; and configure the system for RADIUS auditing and authentication of system users (see "Configuring administrative settings" (page 281)).
user	Accesses the **User** menu, in order to manage users and passwords (see "Managing system users and groups" (page 211)).
distrace	Permanently disables the **/cfg/domain #/server/trace/ssldump** and **/cfg/domain #/server/trace/tcpdump** commands (see "Tracing SSL traffic" (page 99)). The **distrace** command is used to improve security. The only way to reverse this command is to do a boot install.

Configuring the Nortel SNAS host

To configure basic TCP/IP properties for a particular Nortel SNAS device in the cluster, use the following command:

/cfg/sys/host <host ID>

where

host ID is an integer automatically assigned to the host when you perform initial setup on the Nortel SNAS device.

The **/cfg/sys/host <host ID>** command also allows you to halt, reboot, or delete the specified Nortel SNAS device.

The **Cluster Host** menu appears.

The **Cluster Host** menu includes the following options:

/cfg/sys/host <host ID> **followed by:**	
ip <IPaddr>	Sets the Real IP address (RIP) for Interface 1 on the device. The RIP is the Nortel SNAS device host IP address for network connectivity and must be unique on the network. For more information, see "About the IP addresses" (page 42). Changing the RIP using this command does not affect the MIP for the cluster.
sysName <name>	Assigns a name to the managed Nortel SNAS host. The name is a useful mnemonic when managing the Nortel SNAS using SNMP.
sysLocatio <location>	Identifies the physical location of the managed Nortel SNAS host. The location description is a useful mnemonic when managing the Nortel SNAS using SNMP.
license <key>	Installs the license key for the type of license you have purchased. The Nortel SNAS SSL (portal and Nortel SNAS domain client access) license is available for 100, 250, 500, and 1000 users. • **key** is text you paste in. The license key text is supplied to you by Nortel Technical Support. When pasting, ensure you include the BEGIN LICENSE and END LICENSE lines. To obtain a license key, first use the **/info/local** command to find out the MAC address of the Nortel SNAS device. Then provide the MAC address to Nortel Technical Support and request the key for the desired license type.
gateway <IPaddr>	Sets the default gateway address for the device. The default gateway is the IP address of the interface on the core router that will be used if no other interface is specified. To specify a default gateway for Interface 1 traffic, use the **/cfg/sys/host #/interface #/ gateway** command (see "Configuring host interfaces" (page 268)).

`/cfg/sys/host <host ID>` **followed by:**	
`routes`	Accesses the **Host Routes** menu, in order to manage static routes for the Nortel SNAS when there is more than one interface (see “Configuring static routes” (page 270)).
`interface <interface number>`	Accesses the **Host Interface** menu, in order to configure an IP interface (see “Configuring host interfaces” (page 268)).
`port`	Accesses the **Host Port** menu, in order to configure port properties (see “Configuring host ports” (page 271)).
`ports`	Lists the physical ports on the device, by port number. Ports that can exist on the same network (for failover or trunking) are listed together, separated by a comma (,). A port that cannot exist on the same network as other listed ports appears after a colon (:). For example: `Ports = 1,2:3`
`hwplatform`	the hardware platform of the Nortel SNAS device.
`halt`	Stops Nortel SNAS processing. Always use this command before turning off the device. If the Nortel SNAS you want to halt has become isolated from the cluster, you will receive an error message when executing the `halt` command. In this case, log on to the Nortel SNAS using a console connection or remotely by connecting to the Nortel SNAS RIP (host address). Then use the `/boot/halt` command (see "halt" (page 362)).

/cfg/sys/host <host ID> **followed by:**	
reboot	Reboots the Nortel SNAS. If the Nortel SNAS you want to reboot has become isolated from the cluster, you will receive an error message when executing the **reboot** command. In this case, log on to the Nortel SNAS using a console connection or remotely by connecting to the Nortel SNAS RIP (host address). Then use the **/boot/reboot** command (see "reboot" (page 362)).
delete	Removes the Nortel SNAS host from the cluster and resets the device to its factory default configuration. Other Nortel SNAS devices in the cluster are not affected. To ensure that you remove the intended Nortel SNAS, first use the **/cfg/sys/host #/cur** command to view current settings and verify that it is the correct host. (To view information for all Nortel SNAS devices in the cluster, use the **/cfg/sys/cur** command.) After you have removed the Nortel SNAS from the cluster, you must use a console connection to access the device. Log on as the admin user with the admin password to enter the Setup utility. **ATTENTION** If there are other Nortel SNAS devices in the cluster configuration, you cannot delete a device if it is the only Nortel SNAS in the cluster whose status is up. In this case, you will receive an error message when executing the **delete** command. To delete a device from the cluster while all the other cluster members are down, log on to the Nortel SNAS using a console connection or remotely by connecting to the Nortel SNAS RIP (host address). Then use the **/boot/delete** command. When the remaining cluster members come back up, connect to the MIP and repeat the command

/cfg/sys/host <host ID> **followed by:**	
	to delete the Nortel SNAS from the cluster configuration (**/cfg/sys/host #/delete**).

Viewing host information

To view the host number and IP address for each Nortel SNAS device in the cluster, use the **/cfg/sys/host <host ID> /cur** command.

Configuring host interfaces

The default IP interface on the Nortel SNAS host is Interface 1. You can create additional interfaces and specify the ports to be assigned to each interface. If you assign more than one port to an interface, you can choose whether the ports will operate in failover or trunking mode.

You can create a maximum of four interfaces on each Nortel SNAS host.

To configure an IP interface and the assignment of physical ports on a particular Nortel SNAS host, use the following command:

/cfg/sys/host <host ID> /interface <interface ID>

where **interface ID** is an integer in the range 1 to 252 that uniquely identifies the interface on the Nortel SNAS host. To configure a new interface, enter an unused interface ID number. To change the configuration of an existing interface, enter the applicable interface ID number.

The **Host Interface** menu appears.

The **Host Interface** menu includes the following options:

/cfg/sys/host #/interface <interface ID> **followed by:**	
ip <IPaddr>	Sets the network address for the interface. (For Interface 1, the network address is the RIP.)
netmask <mask>	Sets the subnet mask for the interface.

/cfg/sys/host #/interface <interface ID> **followed by:**	
gateway <IPaddr>	Sets the default gateway address for the interface. The default gateway is the IP address of the interface on the core router that will be used for management traffic (such as requests to private authentication servers and DNS servers). The default gateway will be used only for Nortel SNAS domains that point to this interface (**/cfg/doamin #/adv/interface**. If no domain points to this interface, the specified gateway will be ignored.
routes	Accesses the **Host Routes** menu, in order to manage static routes for the Nortel SNAS when there is more than one interface (see "Configuring static routes" (page 270)).
vlanid <tag>	Specifies the VLAN tag if packets received by the interface are tagged with a specific VLAN tag ID.
mode failover|trunking	Specifies the mode of operation for the port numbers assigned to this interface. The options are: • **failover**—only one link is active at any given time. If the port with an active link fails, the active link is immediately switched over to one of the other ports configured for the interface. When you select failover mode, you also have the option of specifying a primary port (see **/cfg/sys/host #/interface #/primary**). • **trunking**—active links are sustained on all configured ports simultaneously, in order to increase network throughput. The default is **failover**.
ports	Accesses the **Interface Ports** menu, in order to manage ports for the interface (see "Managing interface ports" (page 272)).

/cfg/sys/host #/interface <interface ID> **followed by:**	
primary <port>	Specifies the primary port in the interface, on which the active link is set up. If the primary port fails, the active link is immediately transferred to a remaining (secondary) port. As soon as the primary port regains functionality, the active link is transferred back to the primary port. • **port** is an integer indicating the port number of the physical port assigned to the interface. The default is 0 (zero). The default value of zero means that the currently active link remains in use until it fails. If the port fails, the link is transferred to another port. The link remains active on the port to which it was transferred, even after the failed port regains functionality. The primary port setting applies only when you have configured more than one port in the interface, and the mode is failover.
delete	Removes the interface from the system configuration.

Configuring static routes

To manage static routes on a cluster-wide level when more than one interface is configured, use the following command:

/cfg/sys/routes

To manage static routes for a particular Nortel SNAS host when more than one interface is configured, use the following command:

/cfg/sys/host <host ID> /routes

where

host ID is an integer automatically assigned to the host when you perform initial setup on the Nortel SNAS device.

To manage static routes for a particular interface, use the following command:

/cfg/sys/host #/interface <interface ID> /routes

where

interface ID is an integer in the range 1 to 252 that uniquely identifies the interface on the Nortel SNAS host.

The system, host, or interface **Routes** menu appears.

When you add a static route to the system, host, or interface configuration, the route is automatically assigned an index number. There are separate sequences of index numbers for routes configured for the cluster, for each host, and for each interface.

The system, host, or interface **Routes** menu includes the following options:

/cfg/sys/[host #[/interface #]/]routes **followed by:**	
list	IP address information for all configured static routes, by index number.
del <index number>	Removes the specified route from the system, host, or interface configuration. • **index number** is the identification number automatically assigned to the route when you added the route to the configuration. To view the index numbers of all configured static routes, use the **list** command.
add <IPaddr> <mask> <gateway>	Adds a static route to the system, host, or interface configuration. • **IPaddr** is the destination IP address. • **mask** is the network mask. • **gateway** is the IP address on the core router. An index number is automatically assigned to the route.

Configuring host ports

To configure the connection properties for a port, use the following command:

/cfg/sys/host #/port <port>

where **port** is an integer in the range 1 to 4 indicating the port number of the physical port on the Nortel SNAS. The port number is the number identifying the port on the back of the Nortel SNAS.

The **Host Port** menu appears.

The **Host Port** menu includes the following options:

/cfg/sys/host #/port <port> **followed by:**	
autoneg on|off	Specifies the Ethernet auto-negotiation setting for the host and NIC port. The options are: • **on**—the port is set to auto-negotiate speed and mode. This is the recommended setting. • **off**—speed and mode are fixed at a specified setting. The default is **on**. When auto-negotiation is on, ensure that the device to which the port is connected is also set to auto-negotiate.
speed <speed>	Sets the speed for the host and NIC port when auto-negotiation is set to **off**. • **speed**—the port speed in megabits per second. The options are 10|100|1000.
mode full|half	Sets the duplex mode for the host and NIC port when auto-negotiation is set to **off**. The options are **full** and **half**. The default duplex mode is **full**.

Managing interface ports

To view and manage the ports assigned to an interface, use the following command:

/cfg/sys/host #/interface <interface ID> /ports

where

interface ID is an integer in the range 1 to 252 that uniquely identifies the interface on the Nortel SNAS host.

The **Interface Ports** menu appears.

The **Interface Ports** menu includes the following options:

/cfg/sys/host #/interface <interface ID> /ports **followed by:**	
list	all ports assigned to the interface.
del <port>	Removes the specified port from the interface. • **port** is the port number of the physical port on the device.
add <port>	Adds a port to be used in the interface. • **port** is the port number of the physical port on the device. To view available port numbers on the Nortel SNAS device, use the **/cfg/sys/host #/ports** command (see "ports" (page 266)).

Configuring the Access List

]The Access List is a cluster-wide list of IP addresses for hosts authorized to access the Nortel SNAS devices by Telnet, SSH, and SREM. You can configure the list to allow access by individual machines or a range of machines on a specific network.

If the Access List is empty, then access is open to any machine.

ATTENTION
Before you join a Nortel SNAS to the cluster, if there are existing entries in the Access List, you must add to the Access List the RIP (host IP address) for Interface 1 of all Nortel SNAS devices in the cluster. You must do this before you perform the join. Otherwise, the devices will not be able to communicate.

For information about enabling Telnet and SSH access, see “Configuring administrative settings” (page 281).

To manage the Access List in order to control Telnet and SSH access to the Nortel SNAS cluster, use the following command:

/cfg/sys/accesslist

The **Access List** menu appears.

The **Access List** menu includes the following options:

/cfg/sys/accesslist **followed by:**	
list	the network address and network mask for all entries in the Access List, by index number.
del <index number>	Removes the specified entry from the list. • **index number** is the identification number automatically assigned to the entry when you added the entry to the list. To view the index numbers of all configured Access List entries, use the **list** command.
add <IPaddr> <mask>	Adds an entry to the Access List. Only those machines listed will be allowed to access the Nortel SNAS through Telnet or SSH. • **IPaddr** is the IP address of the host to be allowed access. • **mask** is the subnet mask. You can set the mask to specify a single machine or a range of machines on a specific network. An index number is automatically assigned to the entry.

Configuring date and time settings

To configure date and time settings for the cluster, use the following command:

/cfg/sys/time

The **Date and Time** menu appears.

The **Date and Time** menu includes the following options:

/cfg/sys/time **followed by:**	
date <date>	Sets the system date. • **date** is the date in YYYY-MM-DD format.
time <time>	Sets the system time. • **time** is the time in HH:MM:SS format, using a 24-hour clock.

/cfg/sys/time **followed by:**	
tzone	Specifies the time zone. You are prompted to enter a continent or ocean area, a country, and a region (if applicable). To view available input options, press **Enter** to accept the default (`select`) in order to display selection menus for each item.
ntp	Accesses the **NTP Servers** menu, in order to manage NTP servers used by the cluster (see "Managing NTP servers" (page 275)).

Managing NTP servers

You can add NTP servers to the system configuration to enable the NTP client on the Nortel SNAS to synchronize its clock. To compensate for discrepancies, it is recommended that NTP have access to at least three NTP servers.

To manage NTP servers used by the system, use the following command:

/cfg/sys/time/ntp

The **NTP Servers** menu appears.

The **NTP Servers** menu includes the following options:

/cfg/sys/time/ntp **followed by:**	
list	IP address information for all NTP servers configured for the system, by index number.
del <index number>	Removes the specified NTP server from the system configuration. • **index number** is the identification number automatically assigned to the server when you added the server to the configuration. To view the index numbers of all configured NTP servers, use the **list** command.
add <IPaddr>	Adds an NTP server to the system configuration. • **IPaddr** is the IP address of the NTP server. An index number is automatically assigned to the server.

Configuring DNS servers and settings

To configure DNS settings for the cluster, use the following command:

/cfg/sys/dns

The **DNS Settings** menu appears.

The **DNS Settings** menu includes the following options:

/cfg/sys/dns **followed by:**	
servers	Accesses the **DNS Servers** menu, in order to manage servers configured for the cluster (see "Managing DNS servers" (page 277)).
cachesize <entries>	Specifies the size of the local DNS cache. • **entries** is an integer in the range 0–10000 indicating the maximum number of DNS entries in the local DNS cache. The default is 1000.
retransmit <interval>	Sets the interval for retransmitting a DNS query. • **interval** is a positive integer that indicates the time interval in seconds (s), minutes (m), hours (h), or days (d). If you do not specify a measurement unit, seconds is assumed. The default is 2 (2 seconds).
count <count>	Specifies the number of retries. • **count** is a non-negative integer that indicates the maximum number of times a DNS query is retransmitted. The default is 3.
ttl <ttl>	Specifies the maximum time to live (TTL) value for entries in the DNS cache. After the TTL has expired, the entries are discarded. • **ttl** is a non-negative integer that indicates the TTL value in seconds (s), minutes (m), hours (h), or days (d). You can enter compound values (for example, 2h30m). If you do not specify a measurement unit, seconds is assumed. The default is 3h (3 hours).

/cfg/sys/dns **followed by:**	
health <interval>	Sets the interval for the Nortel SNAS to check the health of the DNS servers. At the specified interval, the Nortel SNAS performs a DNS query to each DNS server in the system configuration to determine its health status. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), hours (h), or days (d). If you do not specify a measurement unit, seconds is assumed. The default is 10 (10 seconds).
hdown <count>	Sets the health check down counter. • **count** is a positive integer that indicates the number of times a DNS server health check can time out before the Nortel SNAS determines the DNS server is down. The default is 2.
hup <count>	Sets the health check up counter. • **count** is a positive integer that indicates the number of times a DNS server health check returns a positive response before the Nortel SNAS determines the DNS server is up. The default is 2.

Managing DNS servers

You can add up to three DNS servers to the system configuration. The DNS server is used by the captive portal when it forwards queries on the Exclude List. (For more information about the captive portal and the Exclude List, see "Captive portal and Exclude List" (page 228).)

To configure the cluster to use external DNS servers, use the following command:

/cfg/sys/dns/servers

The **DNS Servers** menu appears.

The **DNS Servers** menu includes the following options:

/cfg/sys/dns/servers **followed by:**	
list	Lists the IP addresses of currently configured DNS servers, by index number.
del <index number>	Removes the specified DNS server from the system configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured DNS servers, use the **list** command.
add <IPaddr>	Adds a DNS server to the system configuration. • **IPaddr**—the IP address of the DNS server The system automatically assigns the next available index number to the server. You can add up to three DNS servers to the configuration.
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of DNS servers in the configuration. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the DNS server you are adding The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of DNS servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured DNS servers, use the **list** command.

Configuring RSA servers

To configure the symbolic name for the RSA server and import the sdconf.rec configuration file, use the following command:

/cfg/sys/rsa

The RSA Servers menu appears.

ATTENTION
This feature is not supported in Nortel Secure Network Access Switch Software Release 1.6.1.

The RSA Servers menu includes the following options:

/cfg/sys/rsa **followed by:**	
rsaname <name>	Sets the symbolic name of the RSA server.
import <protocol> <server> <filename> [<FTP user name> <FTP password>]	Imports a copy of the **sdconf.rec** file from the specified TFTP/FTP/SCP/SFTP server. • **protocol** is the import protocol. Options are **tftp** | **ftp** | **scp** | **sftp**. • **server** is the host name or IP address of the server. • **filename** is the name of the **sdconf.rec** file on the server. The **sdconf.rec** file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/Server administrator to obtain the file and make it available on the specified TFTP/FTP/SCP/SFTP server.
rmnodesecr	Removes the RSA node secret, if necessary. Authentication will then fail until the **Node secret created** check box is unchecked in the **Edit Agent Host** window on the RSA server.
del	Deletes the current RSA server information.

Configuring syslog servers

The Nortel SNAS software can send log messages to specified syslog hosts.

For descriptions of the log messages that the Nortel SNAS can send to a syslog host, see “Syslog messages” (page 451).

To configure syslog servers for the cluster, use the following command:

/cfg/sys/syslog

The **Syslog Servers** menu appears.

The **Syslog Servers** menu includes the following options:

/cfg/sys/syslog **followed by:**	
list	Lists the IP addresses and facility numbers of all configured syslog servers, by index number.
del <index number>	Removes the specified syslog server from the system configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured syslog servers, use the **list** command.
add <IPaddr> <facility>	Adds a syslog server to the system configuration. You are prompted to enter the following information • **IPaddr**—the IP address of the syslog server • **facility**—the local facility number, to uniquely identify syslog entries. For more information about the local facility number, see the manual page for **syslog.conf** under UNIX. The system automatically assigns the next available index number to the server.
insert <index number> <IPaddr> <facility>	Assigns a specific index number to the syslog server you add. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the syslog server you are adding • **facility**—the local facility number, to uniquely identify syslog entries. For more information about the local facility number, see the manual page for **syslog.conf** under UNIX.

/cfg/sys/syslog **followed by:**	
	The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of syslog servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured syslog servers, use the **list** command.

Configuring administrative settings

Administrative settings control the functioning of the CLI. Important administrative settings include:

- enabling Telnet access to the CLI
- enabling SSH access to the CLI (required in order to use the SREM)
- enabling SRS administration to configure the Nortel Health Agent SRS rules (see “Enabling TunnelGuard SRS administration” (page 284))
- setting CLI idle timeout

To configure administrative settings for the system, use the following command:

/cfg/sys/adm

The **Administrative Applications** menu appears.

The **Administrative Applications** menu includes the following options:

/cfg/sys/adm **followed by:**	
snmp	Accesses the **SNMP** menu, in order to configure network management of the cluster (see).
sonmp on|off	Enables or disables support for SynOptics Network Management Protocol (SONMP) network topology information. The default is disabled (**off**).
clitimeout <interval>	Sets the timeout interval for user inactivity in the CLI. At the end of the timeout period, if there is still no activity, the user is automatically logged out. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), hours (h), or days (d). If you do not specify a measurement unit, seconds is assumed. The range is 300–604800 seconds (5 m–7 d). The default is 600 (10 m). Changes to the timeout value do not take effect until the next logon. When the user is automatically logged out, any unapplied changes are lost. Save your configuration changes regularly by using the global **apply** command.
audit	Accesses the **Audit** menu, in order to configure RADIUS auditing (see “Configuring RADIUS auditing” (page 286)).
auth	Accesses the **Authentication** menu, in order to configure RADIUS authentication of system users (see “Configuring authentication of system users” (page 290)).
abl	Accesses the **Auto Blacklisting** menu.
hardenpass	Accesses the **Harden Password** menu.

/cfg/sys/adm **followed by:**	
telnet on|off	Enables or disables Telnet access for remote management of the system. The options are: • **on**—Telnet access is enabled. If there are no entries in the Access List, all Telnet connections are allowed. If there are any entries in the Access List, only the specified machines are allowed Telnet access. • **off**—All Telnet connections are rejected, including connections from machines in the Access List. The default is **off**. For more information about the Access List, see "Configuring the Access List" (page 273).
ssh on|off	Enables or disables SSH access for remote management of the system. The options are: • **on**—SSH access is enabled. If there are no entries in the Access List, all SSH connections are allowed. If there are any entries in the Access List, only the specified machines are allowed SSH access. • **off**—all SSH connections are rejected, including connections from machines in the Access List. The default is **off**. For more information about the Access List, see "Configuring the Access List" (page 273).
srsadmin	Accesses the **SRS Admin** menu, in order to configure the SRS rules (see "Enabling TunnelGuard SRS administration" (page 284)).
sshkeys	Accesses the **SSH Host Keys** menu, in order to manage SSH keys used by all Nortel SNAS hosts in the cluster in accordance with the Single System Image (SSI) concept (see "Configuring Nortel SNAS host SSH keys" (page 284)).
redist	It affects the switch in all domains. Values: yes and no default: no

Enabling TunnelGuard SRS administration

To create and modify the TunnelGuard Software Requirement Set (SRS) rules, you must use the SREM (see *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*,). Before you can access the Rule Builder utility in the SREM, you must enable support for SRS administration.

It is supported till Nortel Secure Network Access Switch Software Release 1.6.1.

To configure support for managing the SRS rules, use the following command:

`/cfg/sys/adm/srsadmin`

The **SRS Admin** menu appears.

The **SRS Admin** menu includes the following options:

`/cfg/sys/adm/srsadmin` **followed by:**	
`port <port>`	Specifies the TCP port used for communication with the SRS administration server. The default is port 4443.
`ena`	Enables SRS administration, for creating and managing SRS rules.
`dis`	Disables SRS administration. The default is disabled.

Configuring Nortel SNAS host SSH keys

The Nortel SNAS functions as both SSH client (for importing and exporting logs using SFTP) and SSH server for secure management communications between the Nortel SNAS devices in a cluster.

ATTENTION
SCP is not supported.

The SSH host keys are a set of keys to be used by all hosts in the cluster in accordance with the Single System Image (SSI) concept. As a result, connections to the MIP always appear to an SSH client to be to the same host.

During initial setup, there is an option to generate the SSH host keys automatically.

To generate and view the SSH keys used by all hosts in the cluster for secure management communications, use the following command:

/cfg/sys/adm/sshkeys

The **SSH Host Keys** menu appears.

The **SSH Host Keys** menu includes the following options:

/cfg/sys/adm/sshkeys **followed by:**	
generate	Generates new SSH host keys (RSA1, RSA, and DSA) to be used by all hosts in the cluster. Enter **Apply** to apply the change immediately and create the key.
show	the current SSH host keys and corresponding fingerprints for the cluster. The following formats are used: • RSA1 keys—there is no standard format. The format in the CLI output is the OpenSSH implementation, except that the line is wrapped. To fully conform to the OpenSSH implementation, you may need to edit the output back into a single line for use in the key storage of an SSH client. • RSA and DSA keys—the SECSH Public Ke y File Format, as described in Internet Draft `draft-ietf-secsh-publickeyfile`.
knownhosts	Accesses the **SSH Known Host Keys** menu, in order to manage the public SSH keys of remote hosts (see “Managing known hosts SSH keys” (page 285))

Managing known hosts SSH keys

You can paste or import public SSH keys from remote hosts as a convenience, so that you do not get prompted to accept a new key during later use of SCP or SFTP for file or data transfer.

To achieve strict "man in the middle" protection, verify the fingerprint before applying the changes.

To manage the public SSH keys of known remote hosts, use the following command:

/cfg/sys/adm/sshkeys/knownhosts

The **SSH Known Host Keys** menu appears.

The **SSH Known Host Keys** menu includes the following options:

/cfg/sys/adm/sshkeys/knownhosts **followed by:**	
list	Lists the type and fingerprint of the known SSH keys for remote hosts, by index number.
del <index number>	Removes the specified known host SSH key. To view the index numbers of all known host SSH keys, use the **list** command.
add	Allows you to paste in the contents of a key file you have downloaded from the remote host. When prompted, paste in the key, then press **Enter**. Enter an elllipsis (...) to signal the end of the key. Valid formats are as described for the **/cfg/sys/adm/sshkeys/show** command or the native format used by the OpenSSH implementation. If the key has a valid format, you will be prompted for the corresponding host name or IP address. You can provide a comma-separated list of names and IP addresses for the host. The system automatically assigns the next available index number to the known host SSH key.
import <IPaddr>	Allows you to import an SSH key from a remote host. • **IPaddr**—the IP address of the remote host The system automatically assigns the next available index number to the known host SSH key.

Configuring RADIUS auditing

You can configure the Nortel SNAS cluster to include a RADIUS server to receive log messages about commands executed in the CLI or the SREM, for audit purposes.

About RADIUS auditing

An event is generated whenever a system user logs on, logs off, or issues a command from a CLI session. The event contains information about user name and session ID, as well as the name of executed commands. You can configure the system to send the event to a RADIUS server for audit trail logging, in accordance with RFC 2866 (RADIUS Accounting).

If auditing is enabled but no RADIUS server is configured, events will still be generated to the event log and any configured syslog servers.

When you add an external RADIUS audit server to the configuration, the server is automatically assigned an index number. You can add several RADIUS audit servers, for backup purposes. Nortel SNAS auditing will be performed by an available server with the lowest index number. You can control audit server usage by reassigning index numbers (see "Managing RADIUS audit servers" (page 289)).

For information about configuring a RADIUS accounting server to log portal user sessions, see "Configuring RADIUS accounting" (page 110).

About the vendor-specific attributes

The RADIUS audit server uses Vendor-Id and Vendor-Type attributes in combination to identify the source of the audit information. The attributes are sent to the RADIUS audit server together with the event log information.

Each vendor has a specific dictionary. The Vendor-Id specified for an attribute identifies the dictionary the RADIUS server will use to retrieve the attribute value. The Vendor-Type indicates the index number of the required entry in the dictionary file.

The Internet Assigned Numbers Authority (IANA) has designated SMI Network Management Private Enterprise Codes that can be assigned to the Vendor-Id attribute (see http://www.iana.org/assignments/enterprise-numbers).

RFC 2866 describes usage of the Vendor-Type attribute.

Contact your RADIUS system administrator for information about the vendor-specific attributes used by the external RADIUS audit server.

To simplify the task of finding audit entries in the RADIUS server log, do the following:

Step	Action
1	In the RADIUS server dictionary, define a descriptive string (for example, `NSNAS-SSL-Audit-Trail`).
2	Map this string to the Vendor-Type value.

--End--

Configuring RADIUS auditing

To configure the Nortel SNAS to support RADIUS auditing, use the following command:

`/cfg/sys/adm/audit`

The **Audit** menu appears.

The **Audit** menu includes the following options:

`/cfg/sys/adm/audit` **followed by:**	
`servers`	Accesses the **RADIUS Audit Servers** menu, in order to configure external RADIUS audit servers for the cluster (see "Managing RADIUS audit servers" (page 289)).
`vendorid`	Corresponds to the vendor-specific attribute used by the RADIUS audit server to identify event log information from the Nortel SNAS cluster. The default Vendor-Id is 1872 (Alteon).
`vendortype`	Corresponds to the Vendor-Type value used in combination with the Vendor-Id to identify event log information from the Nortel SNAS cluster. The default Vendor-Type value is 2 (Alteon-ASA-Audit-Trail).
`ena`	Enables RADIUS auditing. The default is disabled.
`dis`	Disables RADIUS auditing. The default is disabled.

Managing RADIUS audit servers

To configure the Nortel SNAS to use external RADIUS audit servers, use the following command:

/cfg/sys/adm/audit/servers

The **RADIUS Audit Servers** menu appears.

The **RADIUS Audit Servers** menu includes the following options:

/cfg/sys/adm/audit/servers **followed by:**	
list	Lists the IP addresses of currently configured RADIUS audit servers, by index number.
del <index number>	Removes the specified RADIUS audit server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured RADIUS audit servers, use the **list** command.
add <IPaddr> <port> <shared secret>	Adds a RADIUS audit server to the configuration. You are prompted to enter the following information: • **IPaddr**—the IP address of the audit server • **port**—the TCP port number used for RADIUS auditing. The default is 1813. • **shared secret**—the password used to authenticate the Nortel SNAS to the audit server The system automatically assigns the next available index number to the server.
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of RADIUS audit servers in the configuration. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the audit server you are adding

/cfg/sys/adm/audit/servers **followed by:**	
	The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of RADIUS audit servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

Configuring authentication of system users

You can configure the Nortel SNAS cluster to use an external RADIUS server to authenticate system users. Authentication applies to both CLI and SREM users.

The user name and password defined on the RADIUS server must be the same as the user name and password defined on the Nortel SNAS. When the user logs on, the RADIUS server authenticates the password. The user group (admin, oper, or certadmin) is picked up from the local definition of the user.

For more information about specifying user names, passwords, and group assignments for Nortel SNAS system users, see “Managing system users and groups” (page 211).

When you add an external RADIUS authentication server to the configuration, the server is automatically assigned an index number. You can add several RADIUS authentication servers, for backup purposes. Nortel SNAS authentication will be performed by an available server with the lowest index number. You can control authentication server usage by reassigning index numbers (see “Managing RADIUS authentication servers” (page 292)).

To configure the Nortel SNAS to support RADIUS authentication of system users, use the following command:

/cfg/sys/adm/auth

The **Authentication** menu appears.

The **Authentication** menu includes the following options:

/cfg/sys/adm/auth **followed by:**	
servers	Accesses the **RADIUS Authentication Servers** menu, in order to configure external RADIUS authentication servers for the cluster (see "Managing RADIUS authentication servers" (page 292)).
timeout <interval>	Sets the timeout interval for a connection request to a RADIUS server. At the end of the timeout period, if no connection has been established, authentication will fail. • **interval** is an integer that indicates the time interval in seconds (s), minutes (m), or hours (h). If you do not specify a measurement unit, seconds is assumed. The range is 1–10000 seconds. The default is 10 seconds.
fallback on|off	Specifies the desired fallback mode. Valid options are: • **on**—if the RADIUS servers are unreachable, the local passwords defined on the Nortel SNAS are used as fallback • **off**—if the RADIUS servers are unreachable, the only way to access the system is to reinstall the software (boot install) The default is **on**. **ATTENTION** With the fallback mode set to on, unwanted access to the Nortel SNAS is possible using a serial cable if the network cable is disconnected and the local password is known.

/cfg/sys/adm/auth **followed by:**	
ena	Enables RADIUS authentication of system users. The default is disabled.
dis	Disables RADIUS authentication of system users. The default is disabled.

Managing RADIUS authentication servers

To configure the Nortel SNAS to use external RADIUS servers to authenticate system users, use the following command:

/cfg/sys/adm/auth/servers

The **RADIUS Authentication Servers** menu appears.

The **RADIUS Authentication Servers** menu includes the following options:

/cfg/sys/adm/auth/servers **followed by:**	
list	Lists the IP addresses of currently configured RADIUS authentication servers, by index number.
del <index number>	Removes the specified RADIUS authentication server from the current configuration. The index numbers of the remaining entries adjust accordingly. To view the index numbers of all configured RADIUS authentication servers, use the **list** command.

/cfg/sys/adm/auth/servers **followed by:**	
add <IPaddr> <port> <shared secret>	Adds a RADIUS authentication server to the configuration. You are prompted to enter the following information: • **IPaddr**—the IP address of the authentication server • **port**—the TCP port number used for RADIUS authentication. The default is 1813. • **shared secret**—the password used to authenticate the Nortel SNAS to the authentication server The system automatically assigns the next available index number to the server.
insert <index number> <IPaddr>	Inserts a server at a particular position in the list of RADIUS authentication servers in the configuration. • **index number**—the index number you want the server to have • **IPaddr**—the IP address of the authentication server you are adding The index number you specify must be in use. The index numbers of existing servers with this index number and higher are incremented by 1.
move <index number> <new index number>	Moves a server up or down the list of RADIUS authentication servers in the configuration. • **index number**—the original index number of the server you want to move • **new index number**—the index number representing the new position of the server in the list The index numbers of the remaining entries adjust accordingly.

Configuration of auto blacklisting

To create the auto blacklisting, use the following command:

cfg/sys/adm/abl

The **Auto Blacklisting** menu appears.

The **Auto Blacklisting** menu includes the following options:

cfg/sys/adm/abl **followed by:**	
users <list> <add> <del>	user names to be monitored. • **list**—lists monitored users. • **add**—adds a user to list, specify the unique user name. • **del**—deletes a user from lists, specify the index number.
hosts <list> <add> <del>	hosts(IPs) to be monitored. • **list**—lists monitored hosts. • **add**—adds a host to list, specify the IP address. • **del**—deletes a host from list, specify the index number.
user_atmpt	Specifies allowed number of failed attempts to a user account. Default value is 10/1h attempts/time period.
host_atmpt	Specifies allowed number of failed login attempts from a host. Default value is 10/1h attempts/timeperiod.
user_purge	Specify time period for purging failed user attempt record. Default value is 2d.
host_purge	Specify time period for purging failed host attempt record. Default value is 2d.
show	Shows the details of failed login attempts of users and hosts

cfg/sys/adm/abl **followed by:**	
clear	Clears all blacklisted users/hosts.
ena	Enables the auto blacklisting.
dis	Disables auto blacklisting.

Configuration of harden password

To configure harden password, use the following command:

```
cfg/sys/adm/hardenpass
```

The **Harden Password** menu appears.

The **Harden Password** menu includes the following options:

cfg/sys/adm/hardenpass **followed by:**	
length	Specify the minimum length of the password. The value ranges from 1 to 511.
lowercase	Specify the minimum number of lower case characters in the password. The value ranges from 1 to 511.
uppercase	Specify the minimum number of upper case characters in the password. The value ranges from 1 to 511.
digits	Specify the minimum number of digits in the password. The value ranges from 1 to 511.

cfg/sys/adm/hardenpass **followed by:**	
others	Specify the minimum number other characters in the password. The value ranges from 1 to 511.
retry	Specify the number of retries to enter the password. The value ranges from 1 to 15.
ena	Enables harden password.
dis	Disables harden password.

Managing certificates

This chapter includes the following topics:

Overview

To use the encryption capabilities of the Nortel SNAS, you must add a key and certificate that conforms to the X.509 standard.

The key and certificate apply to the cluster. It does not matter whether you connect to the Management IP address (MIP) or Real IP address (RIP) of a Nortel SNAS device in order to manage Secure Socket Layer (SSL) certificates. When you add a key and certificate to one Nortel SNAS device in the cluster, the information is automatically propagated to all other devices in the cluster.

The Nortel SNAS can support a maximum of 1500 certificates. However, only one server certificate can be mapped to a portal server at any one time. For information about mapping a certificate to the portal server, see “Configuring SSL settings” (page 102).

If you ran the quick setup wizard during initial setup, a test certificate has been installed and mapped to the Nortel SNAS portal.

You can install new certificates or import or renew existing certificates.

ATTENTION
The Nortel SNAS supports keys and certificates created by using Apache-SSL, OpenSSL, or Stronghold SSL. However, for greater security, Nortel recommends creating keys and generating certificate signing requests from within the Nortel SNAS system using the CLI or SREM. This way, the encrypted private key never leaves the Nortel SNAS and is invisible to the user.

Key and certificate formats

The Nortel SNAS supports importing, saving, and exporting private keys and certificates in a number of standard formats. Table 53 "Supported key and certificate formats" (page 298) summarizes the supported formats.

Table 53
Supported key and certificate formats

Format	Import/Add	Export/Save	Comment
PEM*	Yes	Yes	Encrypts the private key. Combines the private key and certificate in the same file. **ATTENTION** *You must use the PEM format when: • you save keys and certificates by copying • you add a key or certificate by pasting
DER	Yes	Yes	Does not encrypt the private key. Allows you to store the private key and certificate in separate files.
NET	Yes	Yes	Encrypts the private key. Allows you to store the private key and certificate in separate files.
PKCS12 (also known as PFX)	Yes	Yes	Encrypts the private key. Combines the private key and certificate in the same file. Most browsers allow importing a combined key and certificate file in the PKCS12 format.
PKCS7	Yes	No	Certificate only.
PKCS8	Yes	No	Key only (used in WebLogic).
MS IIS 4	Yes	No	Key only (proprietary format).

Table 53
Supported key and certificate formats (cont'd.)

Format	Import/Add	Export/Save	Comment
Netscape Enterprise Server	Yes	No	Key only (proprietary format). Requires conversion. For information about the conversion tool, contact Nortel Technical Support (see "How to get help" (page 21)).
iPlanet Server	Yes	No	Key only (proprietary format). Requires conversion. For information about the conversion tool, contact Nortel Technical Support (see "How to get help" (page 21)).

Creating certificates

The basic steps to create a new certificate are:

Step	Action
1	Generate a Certificate Signing Request (CSR) (see "Generating and submitting a CSR" (page 305)).
2	Send the CSR to a Certificate Authority (CA), such as Entrust or VeriSign, for certification (see "Generating and submitting a CSR" (page 305)).
3	Install the signed certificate on the Nortel SNAS cluster (see "Installing certificates and keys" (page 299)).
4	Map the installed certificate to the Nortel SNAS portal server (see "Configuring SSL settings" (page 102)).

--End--

Installing certificates and keys

There are two ways to install a certificate and key in the Nortel SNAS cluster:

- by pasting (see "Adding a certificate to the Nortel SNAS " (page 310))
- by importing from a TFTP/FTP/SCP/SFTP server (see "Importing certificates and keys into the Nortel SNAS " (page 314))

When you generate the CSR, the private key is created and stored in encrypted form on the Nortel SNAS using the specified certificate number. After you receive the certificate, which contains the corresponding public key, use the same certificate number when you add the certificate to the Nortel SNAS. Otherwise, the private key and the public key in the certificate will not match.

If you do not generate a CSR but obtain the certificate by other means, you must take additional steps to add a private key that corresponds to the public key of the certificate (see “Adding a private key to the Nortel SNAS ” (page 312)).

If you use the certificate index number of an installed certificate when adding a new certificate, the installed certificate is overwritten.

After you have installed the certificate, map it to the Nortel SNAS portal (see “Configuring SSL settings” (page 102)).

Saving or exporting certificates and keys

You can extract copies of certificates and keys to save as backup or to install on another device.

There are two ways to retrieve a certificate and key from the Nortel SNAS cluster:

- by copying (see “Displaying or saving a certificate and key” (page 316))
- by exporting to a TFTP/FTP/SCP/SFTP server (see “Exporting a certificate and key from the Nortel SNAS ” (page 318))

The copy-and-paste method saves the certificate and key in PEM format.

The export method allows you to choose from a variety of file formats. Nortel recommends using the PKCS12 format (also known as PFX). Most web browsers accept importing a combined key and certificate file in the PKCS12 format. For more information about the formats supported on the Nortel SNAS, see “Key and certificate formats” (page 298).

Updating certificates

To update or renew an existing certificate, do not replace the existing certificate by using its certificate number when you generate the CSR or add the new certificate. Rather, keep the existing certificate until you have verified that the new certificate works as designed.

The recommended steps to update an existing certificate are:

Step	Action
1	Check the certificate numbers currently in use to identify an unused certificate number. In the CLI, use the **`/cfg/cur cert`** command. In the SREM, use the **Certificates > Certificates** screen to add a new certificate.

2 Create a new certificate, using an unused certificate number (see "Generating and submitting a CSR" (page 305)).

   a Generate a CSR.

   b Submit the CSR to a CA.

3 When you receive the new, signed certificate, add it to the Nortel SNAS (see "Installing certificates and keys" (page 299)).

4 Map the new certificate to the portal server (see "Configuring SSL settings" (page 102)).

5 After testing to verify that the new certificate works as intended, delete the old certificate.

   In the CLI, use the **`/cfg/cert <old cert ID> /del`** command. In the SREM, use the **Certificates > Certificates** screen to remove the old certificate.

--End--

Managing private keys and certificates

You can perform the following certificate management tasks in the CLI:

- view, validate, and manage certificates and private keys (see "Managing and viewing certificates and keys" (page 302))
- generate requests for signed certificates (see "Generating and submitting a CSR" (page 305))
- add certificates by copy-and-paste (see "Adding a certificate to the Nortel SNAS " (page 310))
- add private keys by copy-and-paste (see "Adding a private key to the Nortel SNAS " (page 312))
- import certificates and private keys (see "Importing certificates and keys into the Nortel SNAS " (page 314))
- save certificates and private keys (see "Displaying or saving a certificate and key" (page 316))
- export certificates and private keys (see "Exporting a certificate and key from the Nortel SNAS " (page 318))
- create a self-signed certificate for testing purposes (see "Generating a test certificate" (page 320))

Roadmap of certificate management commands

The following roadmap lists the CLI commands to configure and manage server certificates for the Nortel SNAS cluster. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
/cfg/cert <cert id>	name <name>
	cert
	key
	gensigned server | client
	request
	sign
	test
	import
	export
	display [<pass phrase>]
	show
	info
	subject
	validate
	keysize
	keyinfo
	del

Managing and viewing certificates and keys

To view basic information about all certificates configured for the Nortel SNAS cluster, use the **/info/certs** command.

To manage private keys and certificates, access the **Certificate** menu by using the following command:

/cfg/cert <cert id>

where

cert id is an integer in the range 1–1500 representing an index number that uniquely identifies the certificate in the system.

If you specify an unused certificate number, the certificate is created.

The **Certificate** menu appears.

The **Certificate** menu includes the following options:

/cfg/cert <cert ID> **followed by:**	
name <name>	Names or renames the certificate, as a mnemonic aid.
cert	Lets you paste the contents of a certificate file from a text editor. For more information, see “Adding a certificate to the Nortel SNAS ” (page 310).
key	Lets you paste the contents of a key file from a text editor. For more information, see “Adding a private key to the Nortel SNAS ” (page 312).
revoke	Accesses the **Revocation** menu. Not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
gensigned server | client	Generates a certificate that is signed using the private key associated with the currently selected certificate. You are prompted to provide the following parameters: <country> <state or province> <locality> <organization> <organizational unit> <common name> <e-mail address> <validity period> <key size> <CA cert true|false> <serial number> <pass phrase> • servergenerates a signed server certificate provided with key use options that are appropriate for server usage. Set the CA cert value to `true` if you plan to issue your own chained server certificates, generating them from the currently generated server certificate.The CA cert value you specify when generating a certificate translates into the X509v3 Basic Constraints property in the generated certificate. To view the properties of a certificate available on the Nortel SNAS, use the **/cfg/cert #/show** command. • client—not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
request	Generates a certificate signing request. For more information, see “Generating and submitting a CSR” (page 305).

/cfg/cert <cert ID> **followed by:**	
sign	Signs a CSR by using the private key associated with the currently selected certificate. You are prompted to paste in the contents of a CSR. Client certificates are not supported in Nortel Secure Network Access Switch Software Release 1.6.1.
test	Generates a self-signed certificate and private key for testing purposes. For more information, see “Generating a test certificate” (page 320).
import	Installs a private key and certificate by downloading it from a TFTP/FTP/SCP/SFTP server. For more information, see “Importing certificates and keys into the Nortel SNAS ” (page 314).
export	Exports the current key and certificate to a TFTP/FTP/SCP/SFTP server in a format you specify. For more information, see “Exporting a certificate and key from the Nortel SNAS ” (page 318).
display [<pass phrase>]	the current key and certificate, in order to save copies as backup or for export to another device. For more information, see “Displaying or saving a certificate and key” (page 316). The **display** command allows you to save private keys and certificates in the PEM format. To save a certificate and key in another format, use the **/cfg/cert #/export** command.
show	detailed information about the certificate, excluding the certificate name.
info	the serial number, the expiration date, and the values specified for the subject part of the current certificate.

/cfg/cert <cert ID> **followed by:**	
subject	detailed information about the subject part of the current certificate. For example: `C/countryName (2.5.4.6) = US` where: • `countryName` is the mnemonic name • `2.5.4.6` is the object identifier (OID) • `US` is the value
validate	Validates that the private key matches the public key in the current certificate.
keysize	the key size of the private key in the current certificate.
keyinfo	information about how the private key associated with the currently selected certificate is protected. For the Nortel SNAS, private keys are protected by the cluster.
del	Removes the current certificate and private key.

Generating and submitting a CSR

To prepare a CSR for submission to a CA, perform the following steps:

Step	Action
1	Access the **Certificate** menu by using the **/cfg/cert <cert id>** command, where: • to generate a CSR for a new certificate, **<cert id>** is an unused certificate number • to generate a CSR to renew an existing certificate, **<cert id>** is the existing certificate number
2	Prepare the CSR. Enter the following command: **/cfg/cert #/request** You are prompted to enter the certificate request information. Table 54 "CSR information" (page 306) explains the required

parameters. The combined length of the parameters cannot exceed 225 bytes.

Table 54
CSR information

Prompt	Description
Country Name (2 letter code):	The two-letter ISO code for the country where the web server is located. For current information about ISO country codes, see http://www.iana.org.
State or Province Name (full name):	The name of the state or province where the head office of the organization is located. Enter the full name of the state or province.
Locality Name (e.g., city):	The name of the city where the head office of the organization is located.
Organization Name (e.g., company):	The registered name of the organization. The organization must own the domain name that appears in the common name of the web server. Do not abbreviate the organization name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?
Organizational Unit Name (e.g., section):	The name of the department or group that uses the secure web server.
Common Name (e.g., your name or your server's hostname):	The name of the web server as it appears in the URL. The name must be the same as the domain name of the web server that is requesting a certificate. If the web server name does not match the common name in the certificate, some browsers will refuse a secure connection with your site. Do not enter the protocol specifier (http://) or any port numbers or pathnames in the common name. Wildcards (such as * or ?) and IP address are not allowed.
E-mail Address:	The user's e-mail address.

Table 54
CSR information (cont'd.)

Prompt	Description
Subject alternative name (blank or comma separated list of URI:<uri>, DNS:<fqdn>, IP:<ip-address>, email:<email-address>):	Specifies alternative information for the subject if you did not provide a Common Name or e-mail address. The required information is a comma-separated list as follows: • `URI:<uri>`, a Uniform Resource Identifier • `DNS:<fqdn>`, the fully qualified domain name • `IP:<ip-address>` • `email:<email-address>`
Generate new key pair (y/n) [y]:	Specifies whether you want to generate a new pair of private and public keys. The default is y (yes). If you are creating a CSR for a new certificate, accept the option to generate a new key pair. If a configured certificate is approaching its expiration date and you want to renew it without replacing the existing key, specify n (no). The CSR will be based on the existing key for the specified certificate number.
Key size [1024]:	The length of the generated key, in bits. The default value is 1024.
Request a CA certificate (y/n) [n]:	Specifies whether to request a CA certificate to use for client authentication. Request a CA certificate if you plan to issue your own server certificates or client certificates, generating them from the requested CA certificate. The default is `n` (no).
Specify challenge password (y/n) [n]:	Specifies a password to be used during manual revocation of the certificate.

3 Generate the CSR.

After you have provided the required information, press **Enter**. The CSR is generated and displayed on the screen.

4 Apply the changes.

The private key is created and stored in encrypted form on the Nortel SNAS using the specified certificate number.

Figure 15 "Generating a CSR" (page 308) shows sample output for the **`/cfg/cert #/request`** command. For more information about the **Certificate** menu commands, see "Managing and viewing certificates and keys" (page 302).

Figure 15
Generating a CSR

```
>> Certificate 2# request
The combined length of the following parameters may not exceed 225
bytes.
Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (eg, city): City
Organization Name (eg, company): Test Company Inc.
Organizational Unit Name (eg, section): test dept
Common Name (eg, your name or your server's hostname):
www.dummyssltesting.com
Email Address: tester@dummyssltesting.com
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, email:<email-address>):
Generate new key pair (y/n) [y]:
Key size [1024]:
Request a CA certificate (y/n) [n]:
Specify challenge password (y/n) [n]:

-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0xD
jAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9jdT
EZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9yYmp
vcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX2rSY
81cgKJODuUreGF3ZnK7RvlRqSV/
TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZOFQKFB5x/Zs9kNMBUmPBokA1/
GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJiwV2LjUvw65EzCLpq5dhq6ZPE
x7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcNAQkHMRYTFEEgY2hhbGxlbmdlIH
Bhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACemSJr8Xuk9PQZPuIPV7iCDG+eWneU
3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+2iQGbTSH0nVeoqn4TJujq96XpIrb
iAFdE1tR7Lmf6oGdrwG8ypfRpp3PmId6lp+HJ2fUGliPYyNtd/
94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----

Use 'apply' to store the private key in the iSD until
the signed certificate is entered.
The private key will be lost unless you 'apply' or
save it elsewhere using 'export'.

>> Certificate 2# apply
Changes applied successfully.
```

5 Save the CSR to a file.

a Copy the entire CSR, including the `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` lines, and paste it into a text editor.

b Save the file with a `.csr` extension. Nortel recommends using a file name that indicates the server on which the certificate is to be used.

6 Save the private key to a file.

If you intend to use the same certificate number when you add the returned certificate to the Nortel SNAS, perform this step only if you want to create a backup copy of the private key.

If you do not intend to use the same certificate number when you add the returned certificate to the Nortel SNAS, you must perform this step in order to create the key file. When you add the returned certificate to the Nortel SNAS using a different certificate number, you will have to associate the private key with the new certificate by pasting or importing the contents of the key file (see "Installing certificates and keys" (page 299)).

a Display the certificate and key (see "Displaying or saving a certificate and key" (page 316)).

b Copy the private key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines, and paste it into a text editor.

c Save the text editor file with a `.pem` extension. Nortel recommends using the same file name that you defined for the `.csr` file (see step 5), so the connection between the two files is obvious.

7 Submit the CSR to a CA such as Entrust or VeriSign.

a In a text editor, open the `.csr` file you created in step 5.

b Copy the entire CSR, including the `-----BEGIN CERTIFICATE REQUEST-----` and -----*END CERTIFICATE REQUEST*-----, lines.

c Use your web browser to access the CA web site and follow the online instructions. The process for submitting the CSR varies with each CA. When prompted, paste the CSR as required in the CA online request process. If the CA requires you to identify a server software vendor whose software you used to generate the CSR, specify *Apache*.

8 The CA processes the CSR and returns a signed certificate. Create a backup copy of the certificate (see "Displaying or saving a certificate and key" (page 316)).

The certificate is ready to be added into the Nortel SNAS cluster (see "Adding a certificate to the Nortel SNAS " (page 310)).

--End--

Adding a certificate to the Nortel SNAS

The following steps describe how to install a certificate (and key, if applicable) using the copy-and-paste method.

The certificate (and key, if applicable) must be in PEM format.

ATTENTION
Nortel recommends performing copy-and-paste operations using a Telnet or SSH client to connect to the MIP. If you use a console connection to connect to one of the Nortel SNAS devices in the cluster, you may find that HyperTerminal under Microsoft Windows is slow to complete copy-and-paste operations.

Step	Action
1	Access the **Certificate** menu by using the **/cfg/cert <cert id>** command, where **<cert id>** is the certificate number. If you obtained the certificate by using the **/cfg/cert #/request** command to generate the CSR, specify the same certificate number as the certificate number you used to generate the CSR. In this way, the private key remains connected to the certificate number, and you do not need to perform an additional step to add the private key. If you obtained the certificate by means other than using the **/cfg/cert #/request** command to generate the CSR, specify a certificate number not used by any other configured certificate. If the private key and the certificate are not contained in the same file, you will have to perform an additional step to add the private key (see “Adding a certificate to the Nortel SNAS ” (page 310)). To view basic information about configured certificates, use the **/info/certs** command. To verify that the current certificate number is not in use by an installed certificate, use the **/cfg/cert #/show** command.
2	Copy the certificate. **a** In a text editor, open the certificate file you received from the CA. **b** Copy the entire contents, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines. If the certificate file contains the private key as well, also include the entire contents of the key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.
3	Add the certificate.

a Enter the following command:

```
/cfg/cert #/cert
```

b Paste the certificate at the command prompt.

c Press **Enter** to create a new line, and then enter an ellipsis (...) to terminate.

d If you are pasting in the private key at the same time, and if the key has been password protected, you are prompted to enter the password phrase. The password phrase required is the one specified when the key was created or exported.

4 Apply the changes.

If you obtained the certificate by using the **`/cfg/cert #/request`** command to generate the CSR and are using the same certificate number, the certificate is now fully installed.

If you obtained the certificate by means other than using the **`/cfg/cert #/request`** command to generate the CSR and are using a new certificate number, you must now add the corresponding private key (see “Adding a private key to the Nortel SNAS ” (page 312)).

Figure 16 "Adding a certificate by pasting" (page 312) shows sample output for the **`/cfg/cert #/cert`** command. For more information about the **Certificate** menu commands, see “Managing and viewing certificates and keys” (page 302).

ATTENTION
Depending on the type of certificate the CA generates (registered or chain), your certificate may be substantially different from the sample output. Be sure to copy and paste the entire contents of the certificate file.

Figure 16
Adding a certificate by pasting

```
>> Certificate 2# cert
Paste the certificate, press Enter to create a new line,
and then type "..." (without the quotation marks) to
terminate.
> -----BEGIN CERTIFICATE-----
> MIIDTDCCArWgAwIBAgIBADANBgkqhkiG9w0BAQQFADB9MQswCQYDVQQG
> EwJzZTEOMAwGA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9sbTEM
> MA>oGA1UEChMDZG9jMQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3c
> uYS5jb20xGTAXBgkqhkiG9w0BCQEWCnR0dEBjY2MuZG4wHhcNMDAxMjI
> yMDkxOTI0WhcNMDExMjIyMDkxOTI0WjB9MQswCQYDVQQGEwJzZTEOMAw
> GA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9sbTEMMAoGA1UEChM
> DZG9jMQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3cuYS5jb20xGTA
> XBgkqhkiG9w0BCQEWCnR0dEBjY2MuZG4wgZ8wDQYJKoZIhvcNAQEBBQA
> DgY0AMIGJAoGBALXym9cIVfHZUZFE1MFi+xefDviIEvilnJAQSSPITnZ
> a69fzGcL3vpQv0NLxNffs1jEw4RPDMKu2rQ9N02EiiJcrCHnaSNZPdwG
> oX39IkEUkANzm3mh2DlP1RfW4ejpNKsG5Tme/e1vFYWXeXXI1oRtdPIa
> VGxK8pvqBEHDXCcJlAgMBAAGjgdswgdgwHQYDVR0OBBYEFJBM3K0KB03
> fpCOVrQCC34hovwM8MIGoBgNVHSMEgaAwgZ2AFJBM3K0KB03fpCOVrQC
> C34hovwM8oYGBpH8wfTELMAkGA1UEBhMCc2UxDjAMBgNVBAgTBWtpc3R
> hMRIwEAYDVQQHEwlzdG9ja2hvbG0xDDAKBgNVBAoTA2RvYzENMAsGA1U
> ECxMEYmx1ZTESMBAGA1UEAxMJd3d3LmEuY29tMRkwFwYJKoZIhvcNAQk
> BFgp0dHRAY2NjLmRuggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQE
> EBQADgYEAm/GKwEyDKCm2qdPt8+pz1znSGNaRTxfK1R0mjtnDGFb0qk+
> Bv7d9YlX+1QTZhxnZZ4JXuWPJS36kAwiirVbOIaIforIVa+IUlo8HUjM
> vxzIqCYPiiDwBcBi3NsvjlFM7i24Q+lvDLE/Ko+x/YEnNukfp3SBXiJq
> Z8WZIvbTCyT4=
> -----END CERTIFICATE-----
> ...
Certificate added.

>> Certificate 2# apply
```

--End--

Adding a private key to the Nortel SNAS

Step	Action
1	Access the **Certificate** menu by using the **`/cfg/cert <cert id>`** command, where **`<cert id>`** is the certificate number. Use the same certificate number you used when pasting the certificate.
2	Copy the contents of the private key file. **a** Locate the file containing the private key. Make sure the key file corresponds with the certificate file you received from the CA. The public key contained in the certificate works in concert with the related private key to handle SSL transactions.

b In a text editor, open the key file.

c Copy the entire contents, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

3 Add the private key.

a Enter the following command:

`/cfg/cert #/key`

b Paste the contents of the key file at the command prompt.

c Press **Enter** to create a new line, and then enter an ellipsis (...) to terminate.

d If the key is password protected, you are prompted to enter the password phrase. The password phrase required is the one you specified when saving or exporting the private key.

4 Apply the changes.

The certificate and private key are now fully installed.

Figure 17 "Adding a private key by pasting" (page 314) shows sample output for the **`/cfg/cert #/key`** command. For more information about the **Certificate** menu commands, see “Managing and viewing certificates and keys” (page 302).

Figure 17
Adding a private key by pasting

```
>> Certificate 2# key
Paste the key, press Enter to create a new line, and then
type "..."(without the quotation marks) to terminate.
> -----BEGIN RSA PRIVATE KEY-----
> Proc-Type: 4,ENCRYPTED
> DEK-Info: DES-EDE3-CBC,2C60C89FEB57A853
>
> MbbLDYlwdbNfXUGHFm10nfRlI+KTnx2Bdx750EaG8HSVV7KrtnsNF/Fs
> z1jFvO/jnKhZfs4zsVrsstrVlqfP1uatg19VyJSEug1ZcCamH59Dcy+U
> NocFWCzR56PHpyZKGXX66jS+6twYdiXQk58URIudkmGXGTYMvBRuVjV2
> 2ZRLyJk41Az5nA6HiDz6GGs6vkCaPFGm263KxmXjy/okNgSJl9QTqJfS
> q7Eh1cIslBReAE9HXGl0Eubb6gVJu+sRmGhS/yGx4vMx98wiMjL37gRt
> XBfDWlu6u0HOPeJxs6fH05fYzmnpwAHj592TDFdsJi5pmrY0NhAeXfuG
> 8mF/T9nEz02ZA8iQGJsaUPfkeBxbZS+umY/R65Okwt1k2RN4RlFnmRWq
> vhHMrHzJuegez/806YazHBv74sOg3KgETRH92z5yvwbgFwmffgb+hai0
> RlRtZgQ4A5kSAFYW37KDq6eJBsZ/m3Que1buMbh8tRxdGpo54+bGqu5b
> 12iLanLnRk57ENQGTgzxOD/1RZIJHqObCY7VDLkK7WZM/LPa0k+bTeAy
> smZa7fu7gvELJF0ivszs3nzm7zT1y0mJ0QX9u9eoW8wpASCAdCC2r2LZ
> t8o9+IWLSZWh5UCIr8qFKGiLrUIx8coIhxSpx/PqEV8KhSRV+0taq0N7
> pJa3TLmO3o80t5966VSFKc3Y35fx9Yk8G+RlSzo4CxooY4bCKsfchnJ9
> 57SJx5vUyh6jjztnuU4iAfeTVCUdF0LXd+NlQ7T7IMFsjjx9SZuuHPZT
> F0KD/WYLx7FfIFIBHDumu6scraYZOaWaJKI5Pw==
> -----END RSA PRIVATE KEY-----
> ...
Enter pass phrase:
Key added

>> Certificate 2# apply
Changes applied successfully.
```

--End--

Importing certificates and keys into the Nortel SNAS

You can import certificates and private keys into the Nortel SNAS using TFTP, FTP, SCP, or SFTP. For information about the formats supported for import, see "Key and certificate formats" (page 298).

To import a certificate and private key into the Nortel SNAS, perform the following steps.

Step	Action
1	Upload the certificate file and key file to the file exchange server.

ATTENTION
You can arrange to include your private key in the certificate file. When the Nortel SNAS retrieves the specified certificate file from the file exchange server, the Nortel SNAS software analyzes the contents and automatically adds the private key, if present.

2 Access the **Certificate** menu by using the **/cfg/cert <cert id>** command, where **<cert id>** is the certificate number.

To install a new certificate, specify an unused certificate number. To replace an installed certificate, specify the installed certificate index number.

To view basic information about all configured certificates, use the **/info/certs** command. To verify that the current certificate number is not in use by an installed certificate, use the **/cfg/cert #/show** command.

3 Import the certificate. Enter the following command:

/cfg/cert #/import

You are prompted to enter the certificate and private key import information. If the private key has been password protected, you are prompted for the correct password phrase as well. Table 55 "Certificate and key import information" (page 315) explains the required parameters.

Table 55
Certificate and key import information

Parameter	Description
Protocol	The file import protocol. The options are TFTP, FTP, SCP, SFTP. The default is TFTP.
Server host name or IP address	The host name or IP address of the file exchange server.
File name	The name of the file on the file exchange server.
[FTP user name and password]	For FTP, SCP, and SFTP, the user name and password to access the file exchange server. The default is `anonymous`. For anonymous mode, the Nortel SNAS uses the following string as the password (for logging purposes): `admin@<hostname>.isd`.
[Pass phrase]	If the key is password protected, the password phrase specified when the key was created or exported. The password phrase must be at least four characters in length.

4 If the private key was not included in the certificate file, repeat step 3 to import the key file, then go to step 5.

5 Apply the changes.

The certificate and private key are now fully installed.

Figure 18 "Adding a certificate and private key by importing" (page 316) shows sample output for the **/cfg/cert #/import**

command. For more information about the **Certificate** menu commands, see “Managing and viewing certificates and keys” (page 302).

Figure 18
Adding a certificate and private key by importing

```
>> Certificate 3# import
Select protocol (tftp/ftp/scp/sftp) [tftp]: ftp
Enter host name or IP address of server: ftp.example.com
Enter filename on server: VIP_1.crt
Retrieving VIP_1.crt from 192.168.128.58
FTP User (anonymous):
Password:admin@hostname/IP.isd
received 2392 bytes
Enter pass phrase:
Key added.
Certificate added.
Use 'apply' to activate changes.

>> Certificate 3# apply
Changes applied successfully.
```

--End--

Displaying or saving a certificate and key

You can display the current certificate and private key and then save copies as backup or for export to another device.

When you display the certificate and private key, you are prompted to protect it with a password phrase. Nortel recommends adding a password phrase, because this adds an extra layer of security.

Save the certificate by copying the certificate section and pasting it into a text editor, then saving the text file with a .PEM extension. Similarly, save the private key by copying the key section and pasting it into a text editor, then saving the text file with a .PEM extension. You can also save both the certificate and the private key in one file, with a .PEM extension.

To save a certificate and key in another format, use the **`/cfg/cert #/export`** command (see “Exporting a certificate and key from the Nortel SNAS ” (page 318)).

To display the current certificate and key or save a copy, perform the following steps.

Step	Action
1	Access the **Certificate** menu by using the **/cfg/cert <cert id>** command, where **<cert id>** is the certificate number of the certificate you wish to copy. To view basic information about all configured certificates, use the **/info/certs** command.
2	Display the private key and certificate. Enter the following command: **/cfg/cert #/display**
3	When prompted, specify whether or not the key will be encrypted. The default is `yes`.
4	When prompted, specify a password phrase if you wish to password protect the private key. The password phrase must contain at least four characters. If you specify a password phrase, the password phrase must be provided on all occasions in future when the private key file is accessed (for example, when adding, importing, or exporting private keys and certificates).
5	Copy the private key, certificate, or both, as required. For the private key, ensure that you include the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines. For the certificate, ensure that you include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.
6	Paste the private key, certificate, or both into a text editor.
7	Save the file with a .PEM extension. Figure 19 "Displaying a private key and certificate" (page 318) shows sample output for the **/cfg/cert #/display** command. For more information about the **Certificate** menu commands, see “Managing and viewing certificates and keys” (page 302).

Figure 19
Displaying a private key and certificate

```
>> Certificate 1# display
Encrypt private key (yes/no) [yes]:
Enter export pass phrase:
Reconfirm export pass phrase:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,87A8DBDA4FD72948

UNmYDWMJ18ogSiPtHlXa9L2jMqMRA5xKq28cZGk2K64jg7dKaQ4Tvjo3ZnqiTDqLdwXrwJJhvdYgsA
vbPh4fZMjPKIeIMGL2cnD3kPWPXoToh022dTxiksUk2gDFc6mlr7OR796J0V9WlrtWuPOk8nGS/QGR
9drgUZguXWZRM68R9HJAonTU45cUeLOh/h2X168Bnt72lb4ZXeCsgiQ4VwhpW0nU/5itD8YiJlqNUS
HTJbPC24V34FtmpmMelht5CYXOtseI2MsasiHNmoEP7RXohLfW7t/utWCN8rh1kj9cKQWIc8b1Hgtl
+9AUGoVkRo9e4OYNk6Qek0S/Hr7Y4lif6dEnVimqM4MbTiKwoSd3hoWV809QObnB80tlueFNpjinm2
qCKPBTydUPWchRgKEAaYnmOYHhZnfS3/8qWHw+VDu9EQW2+KYKrUlGNO6s1SZQ8P97syGWyEcBhG8O
k4+dQ9+0uGAJl9+bic1u0Y7CxJ70hHrOxhujMEo5tJJnTe2p+E5BGMl6KZpkkgowc1D1FbyOy9qxfr
sBqsBAB97VgTGuJPhdhQGLqlag9VblBDYj2ljTNYZCdcx3ZkwCrdhMtviML5O3knyKvdZZqoS6H/Hq
dSHwRF0u/zeX+frBE+atlSi2flRINBXa8TD/B/CI7LjZECrV2aed2i7HFEeP6VQC5jKQbq2k7nzss9
lvBtl1vV9jwFk/37dSY4tRe3ughKYB4hvWrGuvnnshbAJmzcOiYk0OV4zbOL5SFul/P6qm49yiklcJ
1GhZS34hZVcx6GQvu9DUmLwAaVE4X2NwZxA5AlmUsw==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEajCCA9OgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk
NhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAxIDE1OjAyOjQ5
IDIwMDUtMDgtMTIxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdG
luZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMB4XDTA1MDgx
MjIyMDI0OVoXDTA2MDgxMjIyMDI0OVowgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm
lhMRAwDgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAxNTowMjo0OSAyMDA1LTA4
LTEyMRIwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMTF3d3dy5kdW1teXNzbHRlc3RpbmcuY29tMS
kwJwYJKoZIhvcNAQkBFhp0ZXN0ZXJAZHVtbXlzc2x0ZXN0aW5nLmNvbTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAsxrMJKkS3bpgPylTGUzoBA/H9CKrSMEpWxFOTYs262BYaFrk/jLMHwExmUfhyN
M9jugxv5sFG5duLL2bg4jfRawJnZsJ1CC3bY+n8sqPAv4f1Wy46DrYbS9cucOC5v4hu85DlV0oNAB8
8M3F7B6DN0JwhublN3nTv8zpT56keeECAwEAAaOCAXIwggFuMAwGA1UdEwQFMAMBAf8wEQYJYIZIAY
b4QgEBBAQDAgJEMDIGCWCGSAGG+EIBDQQlFiNBbHRlb24vTm9ydGVsIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQU4fQWn5yi7hkDDWXud+2Pl8XWgn8wgewGA1UdIwSB5DCB4YAU4fQWn5yi7h
kDDWXud+2Pl8XWgn+hgcWkgcIwgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRAw
DgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAxNTowMjo0OSAyMDA1LTA4LTEyMR
IwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMTF3d3dy5kdW1teXNzbHRlc3RpbmcuY29tMSkwJwYJ
KoZIhvcNAQkBFhp0ZXN0ZXJAZHVtbXlzc2x0ZXN0aW5nLmNvbYIBADAJBgNVHRIEAjAAMA0GCSqGSI
b3DQEBBAUAA4GBAHhnJNTeShcMqXVPbyZn5V9DRgZvSMOi+fHr7M7rMpEvYYwD5Idga6YCYmZxpcmx
TpPhFsUX5XRXHWNA/e3LzzpDqq0j82k6JrnpwqWLcWe6AeSCsrQF2lFsZy/r0HFQ12hFmRmKMpgElf
LzfJ2eg6oct9lYzUx4m/84FdlQE7mb
-----END CERTIFICATE-----

>> Certificate 1#
```

--End--

Exporting a certificate and key from the Nortel SNAS

You can export certificate files and key files from the Nortel SNAS using TFTP, FTP, SCP, or SFTP. For information about the formats supported for export, see “Key and certificate formats” (page 298).

To export a certificate and key from the Nortel SNAS, perform the following steps.

Step	Action
1	Access the **Certificate** menu by using the **`/cfg/cert <cert id>`** command, where **`<cert id>`** is the certificate number of the certificate you wish to export.

To view basic information about all configured certificates, use the **/info/certs** command.

2 Export the certificate. Enter the following command:

/cfg/cert #/export

You are prompted to enter the certificate and key export information. The file is exported as soon as you have provided all the required information. Table 56 "Certificate and key export information" (page 319) explains the required parameters.

Table 56
Certificate and key export information

Parameter	Description
Protocol	The file export protocol. The options are TFTP, FTP, SCP, SFTP. The default is TFTP.
Server host name or IP address	The host name or IP address of the file exchange server.
Export format	The key and certificate format in which you want to export the key and certificate. Valid options are: • PEM • DER • NET • PKCS12 (also known as PFX) The PEM and PKCS12 formats always combine the private key and certificate in the same file. Nortel recommends using the PKCS12 format. Most web browsers accept importing a combined key and certificate file in the PKCS12 format. The formats have different capabilities regarding private key encryption and the ability to save the key and certificate in separate files. For more information about the formats, see “Key and certificate formats” (page 298).
Export pass phrase	The password phrase to encrypt the private key. The password phrase must be at least four characters in length.
Reconfirm export pass phrase	Re-enter the password phrase for confirmation.

Table 56
Certificate and key export information (cont'd.)

Parameter	Description
Key and certificate file name	The name of the file on the file exchange server. If you are using a format that saves the private key and certificate in the same file, you are prompted for the combined file name. If you are using a format that saves the private key and certificate in separate files, you are prompted separately for the key file name and the certificate file name.
[FTP user name and password]	For FTP, SCP, and SFTP, the user name and password to access the file exchange server. The default is **anonymous**.

Figure 20 "Exporting a certificate and private key" (page 320) shows sample output for the **/cfg/cert #/export** command. For more information about the **Certificate** menu commands, see "Managing and viewing certificates and keys" (page 302).

Figure 20
Exporting a certificate and private key

```
>> Certificate 1# export
Select protocol (tftp/ftp/scp/sftp) [tftp]: ftp
Enter hostname or IP address of server: ftp.example.com

Select the desired export format, enter a pass phrase and
specify the name of the output file.
Enter export format (pem/der/net/pkcs12): pkcs12
Enter export pass phrase: <passphrase>
Reconfirm export pass phrase: <passphrase once again>
Enter name of combined key and certificate file on remote
host: cert.pfx
FTP User (anonymous):
Password:
sent 2392 bytes
```

--End--

Generating a test certificate

You can generate a self-signed certificate and private key for testing purposes.

The certificate is generated immediately after you have provided all the required information. However, the test certificate and key are not activated until you apply the changes.

To generate a test certificate, perform the following steps:

Step	Action
1	Access the **Certificate** menu by using the `/cfg/cert <cert id>` command, where `<cert id>` is an unused certificate number.
2	Generate the test certificate. Enter the following command: `/cfg/cert #/test` You are prompted to enter the following parameters. The combined length of the parameters cannot exceed 225 bytes • country name (2-letter code) • state or province name • locality name • organization name • organizational unit name • common name • e-mail address • subject alternative name • validity period—the default is 365 days • key size—the default is 1024 bits For more information about the parameters, see Table 54 "CSR information" (page 306).
3	Apply the changes.

--End--

Configuring SNMP

This chapter includes the following topics:

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDU), to different parts of a network. The SNMP-compliant agents on the Nortel SNAS devices store data about themselves in Management Information Bases (MIB) and return this data to the SNMP requesters.

There is one SNMP agent on each Nortel SNAS device, and the agent listens to the Real IP address (RIP) of that particular device. On the Nortel SNAS that currently holds the cluster Management IP address (MIP), the SNMP agent also listens to the MIP.

The SNMP agent supports SNMP version 1, version 2c, and version 3. Notification targets (the SNMP managers receiving trap messages sent by the agent) can be configured to use SNMP v1, v2c, and v3. The default is SNMP v2c. You can specify any number of notification targets on the Nortel SNAS.

For information about the MIBs supported on the Nortel SNAS, see “Supported MIBs” (page 477).

Configuring SNMP

To configure SNMP for the Nortel SNAS network, access the **SNMP** menu by using the following command:

```
/cfg/sys/adm/snmp
```

From the **SNMP** menu, you can configure and manage the following:

- general settings for SNMP management of the cluster (see "Configuring SNMP settings" (page 325))
- parameters in the standard SNMPv2 MIB (see "Configuring the SNMP v2 MIB" (page 326))
- monitor, control, and trap community names (see "Configuring the SNMP community" (page 327))
- SNMPv3 users (see "Configuring SNMPv3 users" (page 328))
- SNMP managers (see "Configuring SNMP notification targets" (page 331))
- SNMP monitors and events (see "Configuring SNMP events" (page 332))

Roadmap of SNMP commands

The following roadmap lists the CLI commands to configure SNMP. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`/cfg/sys/adm/snmp`	`ena`
	`dis`
	`versions <v1 | v2c | v3>`
`/cfg/sys/adm/snmp/snmpv2-mib`	`sysContact <contact>`
	`snmpEnable disabled | enabled`
`/cfg/sys/adm/snmp/community/cfg/sys/adm/snmp/community`	`read <name>`
	`write <name>`
	`trap <name>`
`/cfg/sys/adm/snmp/users <user ID>`	`name <name>`
	`seclevel none | auth | priv`
	`permission get | set | trap`
	`authproto md5 | sha`
	`authpasswd <password>`
	`privproto des | aes`

Command	Parameter
	privpasswd <password>
	del
/cfg/sys/adm/snmp/target <target ID>	ip <IPaddr>
	port <port>
	version v1 | v2c | v3
	del
/cfg/sys/adm/snmp/event	addmonitor [<options>] -b <name> <OID> <op> <value>
	addmonitor [<options>] -t <name> <OID> <value and event>
	addmonitor [<options>] -x <name> <OID> [present|absent|changed]
	delmonitor <name>
	addevent [-c <comment>] <name> <notification> [<OID...>]
	delevent <name>
	list

Configuring SNMP settings

To configure SNMP management of the Nortel SNAS cluster, use the following command:

```
/cfg/sys/adm/snmp
```

The **SNMP** menu appears.

The **SNMP** menu includes the following options:

/cfg/sys/adm/snmp **followed by:**	
ena	Enables network management using SNMP. The default is enabled.
dis	Disables network management using SNMP.

/cfg/sys/adm/snmp **followed by:**	
versions <v1|v2c|v3>	Specifies the SNMP versions allowed. Enter one or more of the following options: • **v1**—SNMP version 1 • **v2c**—SNMP version 2c • **v3**—SNMP version 3 To configure support for multiple versions, use a comma to separate the entries. The default is all versions (v1, v2c, v3).
snmpv2-mib	Accesses the **SNMPv2-MIB** menu, in order to configure parameters in the standard SNMP v2 MIB for the system (see "Configuring the SNMP v2 MIB" (page 326)).
community	Accesses the **SNMP Community** menu, in order to configure the community aspects of SNMP monitoring (see "Configuring the SNMP community" (page 327)).
users	Accesses the **SNMP User** menu, in order to manage SNMPv3 users (see "Configuring SNMPv3 users" (page 328)).
target	Accesses the **Notification Target** menu, in order to configure the notification target aspects of SNMP monitoring (see "Configuring SNMP notification targets" (page 331)).
event	Accesses the **Event** menu, in order to create custom monitoring definitions for the objects in the DISMAN-EVENT-MIB (see "Configuring SNMP notification targets" (page 331)).

Configuring the SNMP v2 MIB

To configure parameters in the standard SNMPv2 MIB, use the following command:

```
/cfg/sys/adm/snmp/snmpv2-mib
```

The **SNMPv2-MIB** menu appears.

The **SNMPv2-MIB** menu includes the following options:

/cfg/sys/adm/snmp/snmpv2-mib **followed by:**	
sysContact <contact>	Designates a contact person for the managed Nortel SNAS cluster. • **contact** is a string specifying the designated contact person's name, together with information about how to contact this person.
snmpEnable disabled|enabled	Enables or disables generating authentication failure traps. The default is disabled.

Configuring the SNMP community

To configure the community aspects of SNMP monitoring, use the following command:

/cfg/sys/adm/snmp/community

The **SNMP Community** menu appears.

The **SNMP Community** menu includes the following options:

/cfg/sys/adm/snmp/community **followed by:**	
read <name>	Specifies the monitor community name that grants read access to the MIB. If you do not specify a monitor community name, read access is not granted. The default monitor community name is public.
write <name>	Specifies the control community name that grants read and write access to the MIB. If you do not specify a control community name, neither read nor write access is granted.
trap <name>	Specifies the trap community name that accompanies trap messages sent to the SNMP manager. If you do not specify a trap community name, the sending of trap messages is disabled. The default trap community name is **trap**.

Configuring SNMPv3 users

The Nortel SNAS manages SNMPv3 users based on the User-based Security Model (USM) for SNMP version 3. For more information about USM, see RFC3414.

To manage SNMPv3 users in the Nortel SNAS configuration, use the following command:

`/cfg/sys/adm/snmp/users <user ID>`

where user ID is an integer in the range 1 to 1024 that uniquely identifies the SNMPv3 user in the Nortel SNAS cluster.

When you first create the user, you must enter the user ID. After you have created the user, you can use either the ID or the name to access the user for configuration.

When you first create the user, you are prompted to enter the following parameters:

- user name—a string that uniquely identifies the USM user in the Nortel SNAS cluster. The maximum length of the string is 255 characters. After you have defined a name for the user, you can use either the user name or the user ID to access the **SNMP User** menu.
- security level—the degree of SNMP USM security. Valid options are:
  - **`none`**—SNMP access is granted without authentication.
  - **`auth`**—SNMP user must provide a verified password before SNMP access is granted. You are later prompted to specify the required password (auth password). SNMP information is transmitted in plain text.
  - **`priv`**—SNMP user must provide a verified password before SNMP access is granted, and all SNMP information is encrypted with the user's individual key. You are later prompted to specify the required password (auth password) and encryption key (priv password).

  The default is **`priv`**.
- permission—the USM user's privileges. Valid options are:

— **get**—USM user is authorized to perform SNMP get requests (read access to the MIB).

— **set** — USM user is authorized to perform SNMP set requests (write access to the MIB). Write access automatically implies read access as well.

— **trap**—USM user is authorized to receive trap event messages and alarm messages.

- authentication protocol—the protocol to be used to authenticate the USM user. Valid options are:

  — **md5**

  — **sha**

  The default is **md5**.

- auth password—a string of at least eight characters specifying the password for USM user authentication. The password is required if the security level is set to **auth** or **priv**.
- privacy protocol—the protocol used for encryption. Valid options are:

  — **des**

  — **aes**

  The default is **des**.

- priv password—a string of at least eight characters specifying the USM user's individual encryption key. The password is required if the security level is set to **priv**.

The **SNMP User** menu appears.

The **SNMP User** menu includes the following options:

/cfg/sys/adm/snmp/users <user ID> **followed by:**	
name <name>	Names or renames the USM user. After you have defined a name for the user, you can use either the user name or the user ID to access the **SNMP User** menu. • **name** is a string that must be unique in the cluster. The maximum length of the string is 255 characters.

/cfg/sys/adm/snmp/users <user ID> **followed by:**	
seclevel none | auth | priv	Specifies the degree of SNMP USM security. Valid options are: • **none**—SNMP access is granted without authentication. • **auth**—the SNMP user must provide a verified password before SNMP access is granted. You are later prompted to specify the required password (auth password). SNMP information is transmitted in plain text. • **priv**—the SNMP user must provide a verified password before SNMP access is granted, and all SNMP information is encrypted with the user's individual key. You are later prompted to specify the required password (auth password) and encryption key (priv password). The default is **priv**.
permission get | set | trap	Specifies the USM user's privileges. Valid options are: • **get**—USM user is authorized to perform SNMP get requests (read access to the MIB). • **set**—USM user is authorized to perform SNMP set requests (write access to the MIB). Write access automatically implies read access as well. • **trap**—USM user is authorized to receive trap event messages and alarm messages. Enter the desired permissions, separated by a comma (,).

/cfg/sys/adm/snmp/users <user ID> **followed by:**	
authproto md5 | sha	Specifies the protocol to be used to authenticate the USM user. Valid options are: • **md5** • **sha** The default is **md5**.
authpasswd <password>	Specifies the password for USM user authentication. The password is required if the security level is set to **auth** or **priv**. • **password** is a string that must be at least eight characters long.
privproto des | aes	Specifies the protocol used for encryption. Valid options are: • **des** • **aes** The default is **des**.
privpasswd <password>	Specifies the USM user's individual encryption key. The password is required if the security level is set to **priv**. • **password** is a string that must be at least eight characters long.
del	Removes the USM user from the configuration.

Configuring SNMP notification targets

SNMP managers function as the notification targets for SNMP monitoring.

To configure notification targets, use the following command:

/cfg/sys/adm/snmp/target <target ID>

where

target ID is a positive integer that uniquely identifies the notification target in the cluster.

The **Notification Target** menu appears.

The **Notification Target** menu includes the following options:

/cfg/sys/adm/snmp/target <target ID> **followed by:**	
ip <IPaddr>	Specifies the IP address to which trap messages are sent. • **IPaddr** is the IP address of the SNMP manager.
port <port>	Specifies the TCP port used by the SNMP manager. The default is port 162.
version v1 | v2c | v3	Specifies the SNMP version used by the SNMP manager. Valid options are: • **v1**—SNMP version 1 • **v2c**—SNMP version 2c • **v3**—SNMP version 3 The default is **v2c**.
del	Removes the current SNMP manager from the Nortel SNAS configuration.

Configuring SNMP events

The Nortel SNAS supports three kinds of SNMP monitors, as defined in the DISMAN-EVENT-MIB:

- boolean —checks the value of a monitored object identifier (OID) against a specific value, and triggers an event if the result matches a specified operation.
- threshold —compares a monitored OID against a range of values, and triggers events if the comparison determines that the OID value is rising too quickly, falling too quickly, or falls outside certain boundaries
- existence —checks the condition of a monitored OID to determine if it is present, absent, or changed, and triggers an event if the result matches the specified condition

To configure monitors and events defined in the DISMAN-EVENT-MIB, use the following command:

/cfg/sys/adm/snmp/event

The **event** menu appears.

The **event** menu includes the following options:

/cfg/sys/adm/snmp/event **followed by:**	
addmonitor [<options>] -b <name> <OID> <op> <value>	Adds a boolean monitor and trigger as defined in the DISMAN-EVENT-MIB. Valid **<options>** are: • **-c <comment>**—adds a comment • **-f <frequency>**—the sampling interval, in seconds. The default is 600 (10 minutes). • **-o <OID>**—additional objects to send in the event • **-e <EventName>**—the name of a notification event • **-d <OID>**—the delta discontinuity OID • **-D timeTicks | timeStamp | dateAndTime**—the delta discontinuity type Other parameters are: • **name**—a unique name you assign to the monitor, for identification • **OID**—the object identifier (or symbolic name) to monitor • **op**—the operator. Valid options are: != (not equals), == (equals), <= (less than or equal to), >= (greater than or equal to), < (less than), > (greater than) • **value**—an integer indicating the value against which the operation will be performed

/cfg/sys/adm/snmp/event **followed by:**	
addmonitor [<options>] -t <name> <OID> <value and event>	Adds a threshold monitor and trigger as defined in the DISMAN-EVENT-MIB. Valid **<options>** are: • **-c <comment>**—adds a comment • **-f <frequency>**—the sampling interval, in seconds. The default is 600 (10 minutes). • **-o <OID>**—additional objects to send in the event • **-d <OID>** — the delta discontinuity OID • **-D timeTicks | timeStamp | dateAndTime** — the delta discontinuity type Other parameters are: • **name** — a unique name you assign to the monitor, for identification • **OID** — the object identifier (or symbolic name) to monitor • **value and event**—a combination of an integer and an event condition, where the integer represents the event condition threshold that will trigger notification. Valid combinations are: **<LowVal> FallingEvent** **<HighVal> RisingEvent** **<DeltaLowVal> DeltaFallingEvent** **<DeltaHighVal> DeltaRisingEvent**

/cfg/sys/adm/snmp/event **followed by:**	
addmonitor [<options>] -x <name> <OID> [present|absent| changed]	Adds an existence monitor and trigger as defined in the DISMAN-EVENT-MIB. Valid **<options>** are: • **-c <comment>**—adds a comment • **-f <frequency>**—the sampling interval, in seconds. The default is 600 (10 minutes). • **-o <OID>**—additional objects to send in the event • **-e <EventName>**—the name of a notification event • **-d <OID>**—the delta discontinuity OID • **-D timeTicks|timeStamp|dateAndTime**—the delta discontinuity type Other parameters are: • **name**—a unique name you assign to the monitor, for identification • **OID**—the object identifier (or symbolic name) to monitor • **present|absent|changed**—indicates whether the object being monitored is present, absent, or has changed
delmonitor <name>	Removes the specified monitor from the configuration.
addevent [-c <comment>] <name> <notification> [<OID...>]	Adds a notification event as defined in the DISMAN-EVENT-MIB. • **-c <comment>**—adds a comment (optional) • **name**—a unique name you assign to the event, for identification • **notification**—the OID (or symbolic name) of the notification • **OID...**—additional notification OIDs (optional)

/cfg/sys/adm/snmp/event **followed by:**	
delevent <name>	Removes the specified event from the configuration.
list	configured monitors and events. For monitors, the monitor name, OID, and type. For events, the event name, notification OID, and comment.

Viewing system information and performance statistics

This chapter includes the following topics:

You can view current status information and events for the cluster and for individual Nortel SNAS hosts. You can view AAA performance statistics for the Nortel SNAS cluster as a whole or for individual hosts in the cluster since the system was started.

Viewing system information and performance statistics

To view current information about system status and the system configuration, access the **Information** menu by using the following command:

```
/info
```

To view performance statistics for the cluster and for individual Nortel SNAS hosts, access the **Statistics** menu by using the following command:

```
/stats
```

Roadmap of information and statistics commands

The following roadmap lists the CLI commands to view information and statistics for the cluster. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
/info	certs
	sys
	sonmp
	licenses [<domain ID>]
	kick <user> <addr> <group>
	blacklist <IPv4 Mac address> <blacklist duration>
	domain [<domain ID>]
	switches [<switch IP protocol/version>] [<status>] [<name type>] [<controlled by>] [<active clients>]
	dist [<hostid>]
	ip <domain ID> <IPaddr>
	mac <MACaddr>
	sessions [<domain ID> [<switch ID> [<username-prefix>]]]
	groupsessi [<domain> <switch login> <port type> <user vlan> <source IP/ portal IP> <source Mac/session type>]
	snmp-profi
	switch [<domainid>] [<switchid>]
	contlist [<Exclude buffers+cache from mem util: [yes/no]>]
	local
	ethernet
	ports
/info/dhcp	list, del, and stats
/info/events	alarms
	download <protocol> <server> <filename>
/info/logs	list
	download <protocol> <server> <filename>
/stats/aaa	total
	isdhost <host ID> <domain ID>
	dump
/stats/dump	

Viewing system information

To view current information about system status and the system configuration, use the following command:

```
/info
```

The **Information** menu appears.

The **Information** menu includes the following options:

/info **followed by:**	
certs	information about all installed certificates, including the certificate name, serial number, expiration date, key size, and subject information for each certificate.
sys	information about the current system configuration, including: • for each Nortel SNAS host in the cluster, the Real IP address (RIP), network mask, default gateway address, static routes, and port configuration • system settings such as date and time, DNS settings, Access List, and administrative applications • NTP, DNS, syslog, audit, and other servers For information about configuring the system, see "Configuring system settings" (page 257).
sonmp	SynOptics Network Management Protocol (SONMP) network topology information, including the IP address, MAC address, chassis type, and state of all Nortel SNAS and SONMP-enabled network devices in the system.
licenses [<domain ID>]	information about the global license pool and current usage, by license type and domain. For the Nortel SNAS, SSL is the only type of license. To restrict the display to a specific domain, enter the domain ID as part of the command. **ATTENTION** With Nortel Secure Network Access Switch Software Release 1.6.1, there is only one domain in the system.

/info **followed by:**	
kick <user> <addr> <group>	Allows the operator to log the specified user out of an Nortel SNAS session. You are prompted to enter the following information: Kick user by name. • **name**—a string that uniquely identifies the user. The maximum length of the string is 255 characters. hosts(IP) to be monitored. • **IPv4 or Mac Address**—specify IPv4 or Mac Address. To log out multiple users, enter an asterisk (*) when prompted for the user name. The system lists the currently logged on users, by automatically assigned index number. Enter the index numbers corresponding to the users you wish to log out. Kick group by name. • **name**—a string that uniquely identifies the group. The maximum length of the string is 255 characters. For example, to log out users corresponding to index numbers 1, 2, 3, and 5, enter **1-3,5**.
blacklist <IPv4 Mac address> <blacklist duration>	Blacklists a device using ipv4 or MAC address and set the duration of blacklisting the device. • **IPv4 Mac address**—specify the IPv4 or MAC Address to be blacklisted. • **blacklist duration**—specify the duration to blacklist the device. Range: 1 minute to 31 days (for example: 20m)

/info **followed by:**	
domain [<domain ID>]	information about the domain configuration, such as the portal Virtual IP address (pVIP), Nortel Health Agent settings, authentication schemes, groups, client filters, SSL settings, portal display, network access devices, and SSH key. To restrict the display to a specific domain, enter the domain ID as part of the command. **ATTENTION** With Nortel Secure Network Access Switch Software Release 1.6.1, there is only one domain in the system.
switches [<switch IP protocol/version>] [<status>] [<name type>] [<controlled by>] [<active clients>]	view the switch status information.
dist [<hostid>]	information about the network access devices and pVIP distribution, by domain.
ip <IPaddr>|[option]	Searches the session table based on the specified IP address and information about the client session. You are prompted to provide the domain ID and the IP address. The information includes: the domain ID; the switch ID and port (in slot/port format); the client's user name (MAC address for an IP Phone); the client's current IP address; the source MAC address; the date the client logged on (time is reported if logon was today); the client device type; the client's current VLAN membership; and the Nortel SNAS host IP address (RIP). The options for device type are phone or dynamic PC (dn_pc). The information is the same as that displayed by the **/info/mac** command.

/info **followed by:**	
mac <macaddr>| [option]	session information for a client based on a specified MAC address. You are prompted to provide the MAC address. The information includes: the domain ID; the switch ID and port (in slot/port format); the client's user name (MAC address for an IP Phone); the client's current IP address; the source MAC address; the date the client logged on (time is reported if logon was today); the client device type; the client's current VLAN membership; and the Nortel SNAS host IP address (RIP). The options for device type are phone or dynamic PC (dn_pc). The information is the same as that displayed by the **/info/ip** command.
sessions [<domain ID> <switchid/hub> [<username_prefix>]]	information about currently active sessions. The information for each session includes: the domain ID; the switch ID and port (in slot/port format); the client's user name (MAC address for an IP Phone); the client's current IP address; the source MAC address; the date the client logged on (time is reported if logon was today); the client device type; the client's current VLAN membership; and the portal IP address through which the client logged on. The options for device type are phone or dynamic PC (dn_pc). To restrict the display to a specific domain, enter the domain ID as part of the command. To restrict the display to sessions originating from a specific network access devices, enter the domain ID and switch ID as part of the command. To restrict the display to specific clients, enter the domain ID, switch ID, and user name as part of the command. Use an asterisk (*) after the user name input to specify it as a prefix.
groupsessi <groupname>	information about currently active group sessions.
dhcp [<list> [<addr> <subnet> <all>]] [<del> [<addr> <subnet> <all>]] <stats>	information about local DHCP leases. For information, see "Managing local DHCP leases" (page 122).

/info **followed by:**	
snmp-profi **[<domainid>] [<profileid>]**	information about the configured snmp profile. For information, see "Configuring SNMP Profiles" (page 75)
switch [<domainid>] [<switchid>]	information about the network access devices in a domain, by device. Information includes the switch type, IP address, NSNA communication port, Red VLAN ID, health check settings, SSH key, and switch status. The information is a subset of information displayed by the **/info/domain** command.
contlist [<Exclude buffers+cache from mem util: [yes/no] >]	information about the Nortel SNAS controllers in the cluster. Information includes the RIP, CPU usage, memory usage, and operational status of each device. An asterisk (*) in the MIP column indicates which Nortel SNAS device in the cluster is currently is control of the MIP. An asterisk (*) in the Local column indicates the particular Nortel SNAS device to which you have connected. To exclude buffers and cache from the memory usage reported, enter the command as: **/info/contlist yes**. To include buffers and cache in the memory usage reported, enter the command as: **/info/contlist no**. The default is to include buffers and cache (no).
local	the current software version, hardware platform, up time (since last boot), IP address, and Ethernet MAC address for the particular Nortel SNAS device to which you have connected. If you have connected to the MIP, the information relates to the Nortel SNAS device in the cluster that is currently in control of the MIP.
ethernet	statistics for the Ethernet network interface card (NIC) on the particular Nortel SNAS device to which you have connected. If you have connected to the MIP, the information relates to the Nortel SNAS device in the cluster that is currently in control of the MIP. • RX packets: the total number of received packets • TX packets: the total number of transmitted packets • errors: packets lost due to error

/info **followed by:**	
	• dropped: error due to lack of resources • overruns: error due to lack of resources • frame: error due to malformed packets • carrier: error due to lack of carrier • collisions: number of packet collisions • RX bytes: received packets in bytes • TX packets: transmitted packets in bytes **ATTENTION** A non-zero collision value may indicate incorrect configuration of Ethernet auto-negotiation. For more information, see the **autoneg** command on "autoneg on|off" (page 272) .
ports	the status of the physical ports on the Ethernet network interface card (NIC) on the particular Nortel SNAS device to which you have connected. If you have connected to the MIP, the information displayed relates to the Nortel SNAS device in the cluster that is currently in control of the MIP. For each port, information includes link status (up/down) and the Ethernet auto-negotiation setting (on/off). If the link is up, the information also includes current values for speed (10/100/1000) and duplex mode (half/full). If the link is down and auto-negotiation is set to off, the information includes the configured values for speed and duplex mode.
events	Accesses the **Events** menu, in order to view and download active alarms and logged events (see “Viewing alarm events” (page 344)).
logs	Accesses the **Logs** menu, in order to view and download log files (see “Viewing log files” (page 345)).

Viewing alarm events

To view active alarms, use the following command:

```
/info/events
```

The **Events** menu appears.

The **Events** menu includes the following options:

/info/events **followed by:**	
alarms	all alarms in the active alarm list, by their main attributes: severity level, alarm ID number, date and time when triggered, alarm name, sender, and cause. To alert the operator at system logon, a notice is displayed if there are active alarms. Alarms are also sent as syslog messages.
download <protocol> <server> <filename>	Transmits the event log file from the Nortel SNAS cluster to a file on the specified TFTP/FTP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the export protocol. Options are `tftp|ftp|scp|sftp`. The default is `tftp`. • **server** is the host name or IP address of the server. • **filename** is the name of the destination log file on the file exchange server.

Viewing log files

To view and download log files, use the following command:

/info/logs

The **Logs** menu appears.

The **Logs** menu includes the following options:

/info/logs **followed by:**	
list	a list of all log files.
download <protocol> <server> <filename>	Transmits the log file from the Nortel SNAS cluster to a file on the specified TFTP/FTP/SFTP file exchange server. You are prompted to provide the following information: • **protocol** is the export protocol. Options are tftp|ftp|scp|sftp. The default is tftp. • **server** is the host name or IP address of the server. • **filename** is the name of the destination log file (*.log.x) on the file exchange server.

Viewing AAA statistics

You can view authentication statistics for the Nortel SNAS cluster as a whole or for one specific Nortel SNAS host in the cluster.

For each configured authentication method and authentication server, the following information :

- the number of authentication requests accepted and rejected
- for external LDAP and RADIUS servers, the number of authentication requests timed out
  The external LDAP and RADIUS servers are listed by IP address and TCP port number.

The CLI reports statistics for all authentication methods configured in the cluster, whether or not they have been included in the authentication order scheme (see “Specifying authentication fallback order” (page 209)). If the statistics for a particular authentication method are always a row of zeroes, this might be because the method is not included in the authentication order scheme.

To view authentication statistics for the Nortel SNAS cluster or for individual Nortel SNAS hosts, use the following command:

```
/stats/aaa
```

The **AAA Statistics** menu appears.

The **AAA Statistics** menu includes the following options:

/stats/aaa **followed by:**	
total	authentication statistics by domain for all Nortel SNAS hosts in the cluster since the system was started.
isdhost <host ID> <domain ID>	authentication statistics for the specified Nortel SNAS host in the cluster since the system was started. You are prompted to specify: • **<host ID>**—the index number automatically assigned to the Nortel SNAS host when you performed the initial setup. • **<domain ID>**—the index number automatically assigned to the Nortel SNAS domain when you created it. To view statistics for all domains, enter 0. **ATTENTION** With Nortel Secure Network Access Switch Software Release 1.6.1, there is only one domain in the system.
dump	Dumps all authentication statistics in the CLI, presenting them first by domain and then by Nortel SNAS host. The display includes the number of accepted and rejected requests for all configured authentication methods, as well as the number of accepted and rejected connections by license type (SSL). In the case of the licenses statistics, the value reported as Rejected refers to connections exceeding the allowed number of concurrent users.

Figure 21 "AAA statistics dump" (page 348) shows sample output for the **/stats/aaa/dump** command.

Figure 21
AAA statistics dump

```
>> Main# stats/aaa/dump
Collecting data, please wait...

AAA Statistics:

  LDAP Servers        DOMAIN  Accepted  Rejected  Timedout
  ------------------------------------------------------
  10.0.0.1:389           1        0         0         0

  RADIUS Servers      DOMAIN  Accepted  Rejected  Timedout
-------------------------------------------------------
  192.168.0.1:1645       1        18        3         1

  Local DB            DOMAIN  Accepted  Rejected
-----------------------------------------------
                         1        2         0

  Licenses            DOMAIN  Accepted  Rejected
-----------------------------------------------
  SSL                    1        0         0

  Local Auth Stats for host 1

  LDAP Servers        DOMAIN  Accepted  Rejected  Timedout
  ------------------------------------------------------
  10.0.0.1:389           1        0         0         0

  RADIUS Servers      DOMAIN  Accepted  Rejected  Timedout
-------------------------------------------------------
  192.168.0.1:1645       1        14        3         0

  Local DB            DOMAIN  Accepted  Rejected
-----------------------------------------------
                         1        0         0

  Licenses            DOMAIN  Accepted  Rejected
-----------------------------------------------
  SSL                    1        0         0

  Local Auth Stats for host 2

  LDAP Servers        DOMAIN  Accepted  Rejected  Timedout
  ------------------------------------------------------
```

Viewing all statistics

To view all available statistics for the Nortel SNAS cluster, use the following command:

`/stats/dump`

Because the Nortel SNAS collects only AAA statistics, the **/stats/dump** command is equivalent to the **/stats/aaa/dump** command.

Kicking by username or address

To kick by username or address, use the following command:

info/kick

The **Kick** menu appears.

The **Kick** menu includes the following options:

info/kick **followed by:**	
user <name>	Kick user by name. • **name**—a string that uniquely identifies the user. The maximum length of the string is 255 characters.
addr <IPv4 or Mac Address>	hosts(IP) to be monitored. • **IPv4 or Mac Address**—specify IPv4 or Mac Address.
group <name>	Kick group by name. • **name**—a string that uniquely identifies the group.The maximum length of the string is 255 characters.

Nortel SNAS TPS Interface

This supports the blacklisting feature, which allows to configure a time-out value for which the specified user or device is not permitted to connect to the network.

You can blacklist a device using ipv4 or MAC address and set the duration of blacklisting the device.

To blacklist a device, use the following command:

info/blacklist

The **blacklist** menu includes the following options:

info/blacklist **followed by:**	
IPv4 Mac address	Specify the IPv4 or MAC Address to be blacklisted.
blacklist duration	Specify the duration to blacklist the device. Range: 1 minute to 31 days (for example: 20m)

Maintaining and managing the system

This chapter includes the following topics:

You can perform the following activities to manage and maintain the system and individual Nortel SNAS devices:

- maintenance, in order to collect information for troubleshooting and technical support purposes (see “Performing maintenance” (page 353)):
  - Dump log file or system internal status information and send it to a file exchange server.
  - Check connectivity between the Nortel SNAS and all configured gateways, routers, and servers.
  - Start and stop tracing to log information about a client session. You can limit the trace to specific features, such as SSL handshake; authentication method, user name, group, and profile; DNS lookups; and the Nortel Health Agent check.
    You can use the trace feature as a debugging tool (for example, to find out why authentication fails). For sample CLI outputs, see “Trace tools” (page 409).
- configuration backup and restore (see “Backing up or restoring the configuration” (page 356))
- software and device management (see “Managing Nortel SNAS devices” (page 361) and “Managing software for a Nortel SNAS device” (page 363)):

— Manage software versions and activate software upgrades.

— Shut down or reboot a particular Nortel SNAS device that has become isolated from the cluster.

— Reset the configuration of a particular Nortel SNAS device back to factory defaults.

Managing and maintaining the system

To perform maintenance activities, access the **Maintenance** menu by using the following command:

```
/maint
```

To manage software versions and Nortel SNAS devices, connect to the particular Nortel SNAS device using Telnet, SSH, or a console connection. Do not connect to the Management IP address (MIP). Access the **Boot** menu by using the following command:

```
/boot
```

Roadmap of maintenance and boot commands

The following roadmap lists the CLI commands to perform maintenance and software and device management activities. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`/maint`	`log <start-log> <stop-log> <displaylog> <clearlog>`
	`dumplogs <protocol> <host name or IP address of server> <filename on server> <collect info from all cluster host?>`
	`dumpstats <protocol> <host name or IP address of server> <filename on server> <collect info from all cluster host?>`
	`chkcfg`
	`starttrace <tags> <domain ID> <output mode>`
	`stoptrace`
`/cfg/ptcfg <protocol> <host name or IP address of server> <filename on server>`	

Command	Parameter
/cfg/gtcfg <protocol> <host name or IP address of server> <filename on server>	
/cfg/dump	
/boot	software
	halt
	reboot
	delete
/boot/software	cur
	activate <version>
	download <protocol> <server> <filename>
	del

Performing maintenance

To check the applied configuration and to download log file and system status information for technical support purposes, use the following command:

/maint

The **Maintenance** menu appears.

The **Maintenance** menu includes the following options:

/maint **followed by:**	
logs<in-memory>	Displays the logging system menu. • **start-log**—starts logging messages into an internal buffer. • **stop-log**—stops logging messages into an internal buffer. • **displaylog**—set to display last n messages, where n is order of 10. • **clearlog**—clears the log messages.

/maint **followed by:**	
dumplogs <protocol> <host name or IP address of server> <filename on server> <collect info from all cluster host?>	Collects system log file information and sends it to a file on the specified file exchange server. The information can then be used for technical support purposes. You are prompted to provide the following parameters if you do not specify them in the command: • **protocol** is the export protocol. Options are `tftp|ftp|sftp`. The default is `tftp`. • **server** is the host name or IP address of the file exchange server. • **filename** is the name of the destination log file on the file exchange server. The file is in gzip compressed tar format. • **all-isds?** specifies whether the information is to be collected from all Nortel SNAS devices in the cluster or only from the device to which you are connected. Valid options are **y** (= yes, all) or **n** (= no, single). If you specify `n` (= no) and you are connected to the MIP, information will be collected for the Nortel SNAS device currently in control of the MIP. • for FTP and SFTP, user name and password. The file sent to the file exchange server does not contain any sensitive information related to the system configuration, such as private keys.
dumpstats <protocol> <host name or IP address of server> <filename on server> <collect info from all cluster host?>	Collects current system internal status information and sends it to a file on the specified file exchange server. The information can then be used for technical support purposes. You are prompted to provide the following parameters if you do not specify them in the command: • **protocol** is the export protocol. Options are `tftp|ftp|sftp`. The default is `tftp`. • **server** is the host name or IP address of the file exchange server. • **filename** is the name of the destination file on the file exchange server. The file is in gzip compressed tar format. • **all-isds?** specifies whether the information is to be collected from all Nortel SNAS devices in the cluster or only from the device to which you are

/maint **followed by:**	
	connected. Valid options are **y** (= yes, all) or **n** (= no, single). If you specify n (= no) and you are connected to the MIP, information will be collected for the Nortel SNAS device currently in control of the MIP. • for FTP and SFTP, user name and password.
chkcfg	Checks if the Nortel SNAS is able to contact gateways, routers, DNS servers, and authentication servers in the system configuration. The command also checks if the Nortel SNAS can connect to web servers specified in group links. The CLI the result of the connectivity check as well as the method used for the check (for example, ping).

	The following is sample output for the **chkcfg** command:
	
	`Checking configuration from 192.168.128.21 0`
	`Testing /cfg/sys/host 1/gateway: 192.168.128.3... ping ok`
	`Testing /cfg/sys/dns/servers: 192.168.128.1... dns ok`
	`All tests completed successfully`

starttrace <tags> <domain ID> <output mode>	Logs information pertaining to a client session. You are prompted to provide the following information: • **tags**—specifies the specific features or subsystems to which you want to limit tracing. The options are: `all`—logs all information. The default is all. `aaa`—logs authentication method, user name, group, and extended profile `dns`—logs failed DNS lookups made during the session `ssl`—logs information related to the SSL handshake procedure (for example, the cipher used) `nha`—logs information related to the Nortel Health Agent check (for example, Nortel Health Agent session status and the SRS rule check result) `snas`—logs operations and events of Nortel SNAS -controlled switches `patchlink`

/maint **followed by:**	

	`radius`
	`nap`
	Enter the desired tag or a comma-separated list of tags (for example, enter **`aaa`** or **`aaa,dns`**). To trace all features, press **Enter** to accept the default.
	• **`domain ID`**—specifies the Nortel SNAS domain to which you want to limit tracing. The default is all. To trace all domains, enter `0` or press **Enter**.
	ATTENTION
	With Nortel Secure Network Access Switch Software Release 1.6.1, there is only one domain in the system.
	• **`output mode`**—options are:
	`interactive`—the information will be logged directly in the CLI when a client authenticates to the portal
	`tftp|ftp|sftp`—the information will be logged to a file exchange server. You are prompted to provide the server information.
	For sample output from the **`starttrace`** command, see "Trace tools" (page 409).

`stoptrace`	Stops tracing. If you selected interactive mode for the **`starttrace`** command and information is logged to the CLI, press **Enter** to redisplay the CLI prompt.

Backing up or restoring the configuration

To save the system configuration to a file on a file exchange server, use the following command:

`/cfg/ptcfg <protocol> <host name or IP address of server> <filename on server>`

ATTENTION
The actual file name in server will be in "NSNAS-<NSNA Version No>-<filename specified in ptcfg comamnd>" format.

To restore the system configuration, use the following command:

`/cfg/gtcfg <protocol> <host name or IP address of server> <filename on server>`

You can also dump the system configuration to the screen and then use copy-and-paste to save it to a text file. To perform a configuration dump, use the following command:

/cfg/dump [<private/secret keys>]

Table 57 "Configuration menu backup and restore commands" (page 357) provides more information about the backup and restore commands on the **Configuration** menu.

Table 57
Configuration menu backup and restore commands

/cfg **followed by:**	
ptcfg <protocol> <host name or IP address of server> <filename on server>	Saves the current configuration, including private keys and certificates, to a file on the specified file exchange server. You can later use this file to restore the configuration by using the **gtcfg** command. You are prompted to provide the following information: • **protocol** is the export protocol. Options are tftp|ftp|scp|sftp. The default is tftp. • **server** is the host name or IP address of the file exchange server. • **filename** is the name of the destination file on the file exchange server. **ATTENTION** If you have fully separated the Administrator user role from the Certificate Administrator user role, the export passphrase defined by the Certificate Administrator is used to protect the private keys in the configuration, and this is transparent to the user. If you later restore the configuration using the **gtcfg** command, the Certificate Administrator must enter the correct passphrase. For more information on separating the Administrator user role from the Certificate Administrator user role, see "Adding a new user" (page 218).

Table 57
Configuration menu backup and restore commands (cont'd.)

/cfg **followed by:**	
gtcfg <protocol> <host name or IP address of server> <filename on server>	Restores a configuration, including private keys and certificates, from a file on the specified file exchange server. You are prompted to provide the following information: • **protocol** is the import protocol. Options are tftp|ftp|scp|sftp. The default is tftp. • **server** is the host name or IP address of the file exchange server. • **filename** is the name of the file on the file exchange server. **ATTENTION** If you have fully separated the Administrator user role from the Certificate Administrator user role, the Certificate Administrator must enter the correct passphrase. The Certificate Administrator defined the passphrase using the **/cfg/sys/user/caphrase** .
dump [<private/secret keys>]	Dumps the current configuration on screen in a format that allows you to restore the configuration without downloading the configuration to a file server. You are prompted to specify if you wish to include private keys in the configuration dump. If you do, then you are prompted to provide a password phrase in order to protect the private keys. The password phrase you specify applies to all private keys. If you later restore the configuration, you will be prompted for this password phrase. Save the configuration to a text file by performing a copy-and-paste operation to a text editor. You can later restore the configuration by using the global **paste** command, at any command prompt in the CLI, to paste the contents of the saved text file. On pasting, the content is batch processed by the Nortel SNAS. To view the pending configuration changes resulting from the batch processing, use the **diff** command. To apply the configuration changes, use the **apply** command.

Configuring the Nortel SNAS scheduler

The Nortel SNAS scheduler allows to run automated system maintenance tasks at scheduled intervals. To configure the Scheduler tasks, use the following command:

/cfg/scheduler

The **Scheduler** menu appears.

The **Scheduler** menu includes the following options:

/cfg/scheduler **followed by:**	
add	Adds task to the scheduler.
del <task number>	Deletes task from scheduler. • **task number**—specify the task number.
list	Lists schedule time details for the following: • Id • Task • Scheduled Time • Comments
ena	Enables the scheduler task.
dis	Disables the scheduler task.

Addition of a scheduled task

To add a scheduled task, use the following command:

/cfg/scheduler/add

This includes the following fields:

/cfg/scheduler/add **followed by:**	
task	Specifies the scheduled task. Values: ptcfg | reboot | starttrace | stoptrace | selftest | upgrade | export
day of week	Select the day of the week. You can select the multiple days in a week. The value ranges from 0 to 6.(Sunday = 0) and [*]: 1-5

/cfg/scheduler/add **followed by:**	
month(s)	Select the month. You can select the multiple months. The value ranges from 1 to 12.
day(s)	Select the day of the month. You can select the multiple days of a month. The value ranges from 1 to 31.
hour(s)	Specify the hour. The value ranges from 0 to 23.
minute(s)	Specify the minute. The value ranges from 0 to 59.
comments	Specify comment for this scheduler task.
protocol	Select the protocol. Values: tftp and ftp.
hostname or IP address	Specify the hostname or IP address of server.
filename	Specify the filename.
password	Password for private keys in cfg.

/cfg/scheduler/add **followed by:**	
starttrace	
day of week	Select the day of the week. You can select the multiple days in a week.The value ranges from 0 to 6. (Sunday = 0) and [*]: 1-5
month(s)	Select the month. You can select the multiple months. The value ranges from 1 to 12. Every Month (*)
day(s)	Select the day of the month. You can select the multiple days of a month. The value ranges from 1 to 31. Every Day (*)
hour(s)	Specify the hour. The value ranges from 0 to 23.
minute(s)	Specify the minute. The value ranges from 0 to 59.
comments	Specify comment for this scheduler.

/cfg/scheduler/add **followed by:**	
output mode	Specify the output mode. Values: tftp, and ftp.
tags	Specify the tag. 1 all, 2 aaa, 3 dhcp, 4 dns, 5 ssl, 6 nha, and 7 snas default is all
domain	Specify the domain.
TFTP Server	Specify the TFTP server.
filename	Specify the filename.

/cfg/scheduler/add **followed by:**	
upgrades	
day of week	Select the day of the week. You can select the multiple days in a week. The value ranges from 0 to 6. (Sunday = 0) and [*]: 1-5
month(s)	Select the month. You can select the multiple months. The value ranges from 1 to 12 .
day(s)	Select the day of the month. You can select the multiple days of a month. The value ranges from 1 to 31.
hour(s)	Specify the hour. The value ranges from 0 to 23.
minute(s)	Specify the minute. The value ranges from 0 to 59.
comments	Specify comment for this scheduler
protocol	Select the Protocol (tftp/ftp).
hostname or IP address	Specify hostname or IP address of server.
filename	Specify the filename.

Managing Nortel SNAS devices

To manage Nortel SNAS software and devices, use the following command:

```
/boot
```

The **Boot** menu appears.

The **Boot** menu includes the following options:

/boot **followed by:**	
software	Accesses the **Software Management** menu, in order to view, download, and activate software versions (see “Managing software for a Nortel SNAS device” (page 363)).
halt	Stops the Nortel SNAS device to which you are connected (using Telnet, SSH, or a console connection). If you have a Telnet or SSH connection to the Management IP address (MIP), use the **/cfg/sys/host #/ halt** command instead (see "halt" (page 266)). **ATTENTION** Always use the **halt** command before turning off the device.
reboot	Reboots the Nortel SNAS device to which you are connected (using Telnet, SSH, or a console connection). If you have a Telnet or SSH connection to the Management IP address (MIP), use the **/cfg/sys/host #/reboot** command instead (see "reboot" (page 267)).
delete	Resets the Nortel SNAS device to which you are connected (using Telnet, SSH, or a console connection) to its factory default configuration. All IP configuration is lost. The software itself remains intact. After executing the **delete** command, you can only access the device using a console connection. Log on as the Admin user (user name: admin, password: admin) to enter the **Setup** Menu. **ATTENTION** If you receive a warning that the device you are trying to delete has no contact with any other master Nortel SNAS device in the cluster, also connect to the MIP (using Telnet or SSH) and delete the Nortel SNAS device from the cluster by using the **/cfg/sys/host #/delete** command (see "delete" (page 268)).

/boot followed by:	
	The **/boot/delete** command is primarily intended for when you want to delete a Nortel SNAS device in one of the following situations : • The device has become isolated from the cluster, • The device has been physically removed from the cluster without first performing the **/cfg/sys/host #/delete** command. In these situations, you must use the **/boot/delete** command to present the **Setup** menu, from which you can perform the **new** and **join** commands.

Managing software for a Nortel SNAS device

To view, download, and activate software versions for the Nortel SNAS device to which you are connected, use the following command:

/boot/software

The **Software Management** menu appears.

The **Software Management** menu includes the following options:

/boot/software followed by:	
cur	the status of the software versions on the particular device to which are connected. The status options are: • permanent—the software version that is currently operational • old—the software version that preceded the currently operational software version • unpacked—the software upgrade package has been downloaded but not yet activated If you activate a software version indicated as either unpacked or old, the status of that version is propagated to permanent. The software status change occurs after the Nortel SNAS device performs a reboot.

/boot/software **followed by:**	
activate <version>	Activates a downloaded software upgrade package that the **cur** command indicates as `unpacked`. If serious problems occur when the new software version runs, you can switch back to the previous version by activating the software version that the **cur** command indicates as `old`. The Nortel SNAS reboots when you confirm the **activate** command. **ATTENTION** When you activate a software upgrade on a Nortel SNAS device, all the Nortel SNAS devices in the cluster reboot. All active sessions are lost.
download <protocol> <server> <filename>	Downloads a new software package from the specified file exchange server, in order to perform a minor or major upgrade. You are prompted to provide the following parameters if you do not specify them in the command: • **protocol** is the import protocol. Options are `tftp|ftp|scp|sftp`. The default is `tftp`. • **server** is the host name or IP address of the file exchange server. • **filename** is the name of the software upgrade package. Software upgrade packages typically have the .pkg file name extension. • for FTP, SCP, and SFTP, user name and password If you include a directory path and file name (separated by a forward slash (/)) on the same line as the FTP server host name or IP address when you run the command, make sure you put the combined directory path and file name string within double quotation marks. For example: `>> Software Management# download ftp 10.0.0.1 "pub/NSNA-5.1.1-upgrade_complete.pkg"` If you are using anonymous mode when downloading the software package from an FTP server, the Nortel SNAS uses the following string as the password (for logging purposes):

/boot/software **followed by:**	
	admin@ <hostname> .isd
del	Removes a software package that has been downloaded but not yet activated (status is `unpacked`). You cannot delete software versions with any other status (see the **cur** command).

Upgrading or reinstalling the software

This chapter includes the following topics:

The Nortel SNAS software image is the executable code running on the Nortel SNAS. A version of the image ships with the Nortel SNAS and is preinstalled on the device. As new versions of the image are released, you can upgrade the software running on your Nortel SNAS. In some cases, you may need to reinstall the software on the Nortel SNAS in order to return the device to its factory defaults.

Upgrading the Nortel SNAS

There are two types of upgrades:

- **Minor release upgrade:** This is typically a bug fix release. All configuration data is retained. To perform a minor upgrade, connect to the Management IP address (MIP) of the cluster you want to upgrade.
  Major release upgrade: This kind of release may contain bug fixes as well as feature enhancements. All configuration data is retained. To perform a major upgrade, connect to the MIP of the cluster you want to upgrade.

ATTENTION
When you activate a software upgrade on a Nortel SNAS device, all the Nortel SNAS devices in the cluster reboot. All active sessions are lost.

Upgrading the software on your Nortel SNAS requires the following:

Step	Action
1	Loading the new software upgrade package or install image onto a TFTP/FTP/SCP/SFTP server on your network.
2	Downloading the new software from the TFTP/FTP/SCP/SFTP server to your Nortel SNAS.
3	Activating the software on the Nortel SNAS.

--End--

ATTENTION
Before upgrading, check the accompanying release notes for any specific actions to take for the particular software upgrade package or install image.

Performing minor and major release upgrades

The following description applies to a minor or a major release upgrade.

To upgrade the Nortel SNAS you will need the following:

- Access to one of your Nortel SNAS devices through a remote connection (Telnet or SSH), or a console connection.
- The software upgrade package, loaded on a TFTP/FTP/SCP/SFTP server on your network.
- The host name or IP address of the TFTP/FTP/SCP/SFTP server. If you choose to specify the host name, note that the DNS parameters must have been configured. For more information, see "Configuring DNS servers and settings" (page 276).
- The name of the software upgrade package (upgrade packages are identified by the **`.pkg`** file name extension).

The set of installed Nortel SNAS devices you are running in a cluster cooperate to give you a single system view. Thus, to perform an upgrade, you only need to connect to the MIP of the cluster. The upgrade will automatically be executed on all the Nortel SNAS devices in operation at the time of the upgrade. All configuration data is retained.

You can access the MIP by a Telnet or an SSH connection.

ATTENTION
Telnet and SSH connections to the Nortel SNAS are disabled by default, after the initial setup has been performed. For more information about enabling Telnet and SSH connections, see "Configuring administrative settings" (page 281).

When you have gained access to the Nortel SNAS, download the software image (see "Downloading the software image" (page 369)).

Downloading the software image

To download the software upgrade package, perform the following steps:

Step	Action

1	Enter the following command at the Main menu prompt. Then select whether to download the software upgrade package from a TFTP/FTP/SCP/SFTP server.
	For some TFTP servers, files larger than 16 MB may cause the upgrade to fail.
	`>> Main# boot/software/download`
	`Select protocol (tftp/ftp/scp/sftp) [tftp]: ftp`

2	Enter the host name or IP address of the server. `Enter hostname or IP address of server:` *<server host name or IP>*

3	Enter the file name of the software upgrade package to download.
	If needed, the file name can be prefixed with a search path to the directory on the TFTP/FTP/SCP/SFTP server.
	If you are using anonymous mode when downloading the software package from an FTP server, the following string is used as the password (for logging purposes): `admin@hostname/IP.isd.`
	`Enter filename on server:` *<filename.pkg>*
	`FTP User (anonymous):` *<username or press ENTER for anonymous mode>*
	`Password:` *<password or press ENTER for default password in anonymous mode>*
	`Received 28200364 bytes in 4.0 seconds`
	
	`Unpacking...`
	`ok`
	`>> Software Management#`

--End--

Activating the software upgrade package

The Nortel SNAS can hold up to two software versions simultaneously. To view the current software status, use the **/boot/software/cur** command. When a new version of the software is downloaded to the Nortel SNAS, the software package is decompressed automatically and

marked as *unpacked*. After you *activate* the unpacked software version (which causes the Nortel SNAS to reboot), the software version is marked as *permanent*. The software version previously marked as *permanent* will then be marked as *old*.

For minor and major releases, the software upgrade occurs in synchronized fashion among the set of Nortel SNAS devices in a cluster. If a Nortel SNAS device in a cluster is not operational when the software is upgraded, it will automatically pick up the new version when it is started.

ATTENTION
If more than one software upgrade has been performed on a cluster while a Nortel SNAS device has been out of operation, the software version currently in use in that cluster must be reinstalled on that Nortel SNAS device. For more information about how to perform a reinstall, see "Reinstalling the software" (page 372).

When you have downloaded the software upgrade package, you can inspect its status with the **`/boot/software/cur`** command.

Step	Action

1 At the `Software Management#` prompt, enter the following command:

```
>> Software Management# cur
Version          Name             Status
-------          ----             ------
x.x              NSNAS            old
z.z              NSNAS            permanent
```

The downloaded software upgrade package is indicated with the status `unpacked`. The software versions can be marked with one out of four possible status values. The meaning of these status values are:

- `unpacked` means that the software upgrade package has been downloaded and automatically decompressed.
- `permanent` means that the software is operational and will survive a reboot of the system.
- `old` means the software version has been permanent but is not currently operational. If a software version marked *old* is available, it is possible to switch back to this version by *activating* it again.
- `current` means that a software version marked as *old* or *unpacked* has been activated. As soon as the system has

performed the necessary health checks, the *current* status changes to *permanent*.

To activate the unpacked software upgrade package, use the **/boot/software/activate** command.

ATTENTION
When you activate a software upgrade on a Nortel SNAS device, all the Nortel SNAS devices in the cluster reboot. All active sessions are lost.

2 At the `Software Management#` prompt, enter:

```
>> Software Management# activate
Enter software version to activate:
Confirm action 'activate'?  [y/n]: y
Activate ok, relogin                    <you are logged out here>
Restarting system.

login:
```

ATTENTION
Activating the unpacked software upgrade package may cause the command line interface (CLI) software to be upgraded as well. Therefore, you will be logged out of the system, and will have to log in again. Wait until the login prompt appears. This may take up to two minutes, depending on your type of hardware platform and whether the system reboots.

3 Log in again and verify the new software version:

```
>> Main# boot/software/cur
Version          Name             Status
-------          ----             ------
x.x              NSNAS            permanent
z.z              NSNAS            old
```

In this example, version x.x is now operational and will survive a reboot of the system, while the software version previously indicated as *permanent* is marked as *old*.

ATTENTION
If you encounter serious problems while running the new software version, you can revert to the previous software version (now indicated as *old*). To do this, *activate* the software version indicated as *old*. When you log in again after having activated the *old* software version, its status is indicated as *current* for a short while. After about one minute, when the system has performed the necessary health checks, the *current* status is changed to *permanent*.

--End--

Reinstalling the software

If you are adding a Nortel SNAS device to an existing cluster, you may need to reinstall the software on the new Nortel SNAS if the software versions on the new Nortel SNAS and the existing Nortel SNAS cluster differ. Otherwise, it is only in the case of serious malfunction that you might need to reinstall the software, and this seldom occurs.

You must perform the reinstall using a console connection.

Reinstalling the software resets the Nortel SNAS to its factory default configuration. The reinstall erases all other configuration data and current software, including old software image versions or upgrade packages that may be stored in the flash memory card or on the hard disk.

Before you begin

To reinstall the software on the Nortel SNAS from an external file server, you require the following:

- access to the Nortel SNAS using a console connection
- an install image, loaded on a TFTP/FTP/SCP/SFTP server on your network
- the IP address of the TFTP/FTP/SCP/SFTP server
- the name of the install image
- authorization to log on as the boot user

ATTENTION
A reinstall wipes out all configuration data, including network settings. Before reinstalling the software on a Nortel SNAS device with a working configuration, save all configuration data to a file on a TFTP/FTP/SCP/SFTP server. If you use the **ptcfg** command in the CLI, the saved configuration data will include installed keys and certificates. You can later restore the configuration, including the installed keys and certificates, by using the **gtcfg** command. (For more information about these CLI commands, see "Backing up or restoring the configuration" (page 356).) If you want to make separate backup copies of your keys and certificates, use the **display** or **export** commands. (For more information about these commands, see "Saving or exporting certificates and keys" (page 300).)

If a software CD was shipped with the Nortel SNAS, you can also reinstall the software from the CD (see "Reinstalling the software from a CD" (page 375)).

Reinstalling the software from an external file server

To reinstall the software image downloaded to an external file server, perform the following steps:

Step	Action
1	Log on as the boot user. The password for the boot user is ForgetMe.

```
login: boot
Password: ForgetMe
*** Reinstall Upgrade Procedure ***
If you proceed beyond this point, the active network
configuration will be reset, requiring a reboot to
restore any current settings.  However, no permanent
changes will be done until the boot image has been
downloaded.
Continue (y/n)?  [y]:
```

Press **Enter** to accept the default (yes) and continue.

2 Specify the network port and IP network settings.

If the Nortel SNAS was previously configured for network access, the previous settings are the suggested default values presented within square brackets. To accept the suggested values, press **Enter**. If the Nortel SNAS was not previously configured for network access, or you deleted the Nortel SNAS from the cluster using the **/boot/delete** command, no suggested values related to a previous configuration are presented within square brackets; you must provide information about the network settings.

a Specify the port for network connectivity.

b If the core router attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

c Specify the host IP address for the device.

d Specify the network mask.

e Specify the default gateway IP address.

```
Select a network port (1-4, or i for info) [1]:
Enter VLAN tag id (or zero for no VLAN tag) [0]:
Enter IP address for this iSD [192.168.128.185]:
Enter network mask [255.255.255.0]:
Enter gateway IP address [192.168.128.1]:
```

3 Specify the download details:

a protocol for the download method

b server IP address

c file name of the boot image

d user name and password, if the server does not support anonymous logon. The default is anonymous.

```
Select protocol (tftp/ftp/scp/sftp) [tftp]:
<protocol>
Enter <protocol> server address: <IPaddr>
Enter file name of boot image: NSNAS-x.x.x-boot.img
Enter FTP Username [anonymous]:
Password:
Downloading boot image...
Installing new boot image...
Done
```

ATTENTION
For some TFTP servers, files larger than 16 MB may cause the update to fail.

4 Wait for the Nortel SNAS to reboot on the newly installed boot image.

```
Restarting...
Restarting system.
Alteon WebSystems, Inc.  0004004C
Booting...
Login:
```

5 Log on as the admin user to enter the **Setup** menu and perform the initial setup of the Nortel SNAS device (see "Initial setup" (page 41)).

--End--

Reinstalling the software from a CD

To reinstall the software image from a CD, perform the following steps:

Step	Action
1	Boot the Nortel SNAS from the CD.
2	Log on as the root user (no password).
3	Run **`install-nsnas isd4050`**.
4	When the installation is complete, remove the CD and reboot.

--End--

The Command Line Interface

This chapter explains how to access the Nortel SNAS through the Command Line Interface (CLI).

This chapter includes the following topics:

The Nortel SNAS software provides means for accessing, configuring, and viewing information and statistics about the Nortel SNAS configuration. By using the built-in, text-based command line interface and menu system, you can access and configure the Nortel SNAS or cluster either through a local console connection (using a computer running terminal emulation software) or through a remote session using a Telnet client or a Secure Shell (SSH) client.

When using a Telnet or SSH client to connect to a cluster of Nortel SNAS devices, always connect to the Management IP address (MIP). Configuration changes are automatically propagated to all members of the cluster. However, to use the **`/boot/halt`**, **`/boot/reboot`**, or **`/boot/delete`** commands, connect to the Real IP address (RIP) of the particular Nortel SNAS device on which you want to perform these commands, or connect to that Nortel SNAS with a console connection.

Connecting to the Nortel SNAS

You can access the CLI in two ways:

- using a console connection through the console port (see “Establishing a console connection” (page 378))
- using a Telnet connection or SSH connection over the network (see “Establishing a Telnet connection” (page 379) or “Establishing a connection using SSH” (page 380))

Establishing a console connection

Use a console connection to perform the initial setup and when reinstalling the Nortel SNAS software as the boot user. You must also use a console connection when logging in as root user for advanced troubleshooting purposes.

Requirements

To establish a console connection with the Nortel SNAS, you need the following:

- An ASCII terminal or a computer running terminal emulation software set to the parameters shown in Table 58 "Console configuration parameters" (page 378):

Table 58
Console configuration parameters

Parameter	Value
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- A serial cable with a female DB-9 connector. For more specific information, see the chapter about connecting to the Nortel SNAS in *Nortel Secure Network Access Switch 4050 Installation Guide* , (NN47230-300).

Procedure steps

Step	Action
1	Connect the terminal to the Console port using the correct serial cable.

When connecting to a Nortel SNAS, use a serial cable with a female DB-9 connector (shipped with the Nortel SNAS).

2 Power on the terminal.

3 To establish the connection, press ENTER on your terminal.

--End--

You will next be required to log on by entering a user name and a password. For more information on user accounts and default passwords, see "Accessing the Nortel SNAS cluster" (page 381).

Establishing a Telnet connection

A Telnet connection offers the convenience of accessing the Nortel SNAS cluster from any workstation connected to the network. Telnet access provides the same options for user access and administrator access as those available through the console port.

When you use a Telnet connection to access the Nortel SNAS from a workstation connected to the network, the communication channel is not secure. All data flowing back and forth between the Telnet client and the Nortel SNAS is sent unencrypted (including the password), and there is no server host authentication.

To configure the Nortel SNAS cluster for Telnet access, you need to have a device with Telnet client software located on the same network as the Nortel SNAS device or cluster. The Nortel SNAS must have a RIP and a MIP. If you have already performed the initial setup by selecting **`new`** or **`join`** in the Setup menu, the assignment of IP addresses is complete.

When you are making configuration changes to a cluster of Nortel SNAS devices using Telnet, Nortel recommends that you connect to the MIP. However, if you want to halt or reboot a particular Nortel SNAS in a cluster, or reset all configuration to the factory default settings, you must connect to the RIP (the IP address of the particular Nortel SNAS device). To view the IP addresses of all Nortel SNAS devices in a cluster, use the **`/info/contlist`** command.

ATTENTION
Telnet/ssh will be enabled on RIP & MIP.

Enabling and restricting Telnet access

Telnet access to the Nortel SNAS cluster is disabled by default, for security reasons. However, depending on the severity of your security policy, you may want to enable Telnet access. You may also restrict Telnet access to one or more specific machines.

For more information on how to enable Telnet access, see the **/cfg/sys/adm/telnet** command (see "telnet on|off" (page 283)). For more information on how to restrict Telnet access to one or more specific machines, see “Configuring the Access List” (page 273).

Running Telnet

Once the IP parameters on the Nortel SNAS are configured and Telnet access is enabled, you can access the CLI using a Telnet connection. To establish a Telnet connection with the Nortel SNAS, run the Telnet program on your workstation and issue the Telnet command, followed by the IP address of the Nortel SNAS.

```
telnet <IP address>
```

You will then be prompted to enter a valid user name and password. For more information about different user accounts and default passwords, see “Accessing the Nortel SNAS cluster” (page 381).

Establishing a connection using SSH

Using an SSH client to establish a connection over the network provides the following security benefits:

- server host authentication
- encryption of passwords for user authentication
- encryption of all traffic that is transmitted over the network when configuring or collecting information from the Nortel SNAS

Enabling and restricting SSH access

SSH access to the Nortel SNAS is disabled by default. However, depending on the severity of your security policy, you may want to enable SSH access. You may also restrict SSH access to one or more specific machines.

For more information on how to enable SSH access, see the **/cfg/sys/adm/ssh** command (see "ssh on|off" (page 283)). For more information on how to restrict SSH access to one or more specific machines, see “Configuring the Access List” (page 273).

Running an SSH client

Connecting to the Nortel SNAS using an SSH client is similar to connecting using Telnet: the IP parameters on the Nortel SNAS must be configured in advance, and SSH access must be enabled. After you provide a valid user name and password, the CLI in the Nortel SNAS is accessible the same way as when using a Telnet client. However, since a secured and encrypted communication channel is set up even before the user name and password is transmitted, all traffic sent over the

network while configuring or collecting information from the Nortel SNAS is encrypted. For information about different user accounts and default passwords, see “Accessing the Nortel SNAS cluster” (page 381).

During the initial setup of the Nortel SNAS device or cluster, you are provided with the choice to generate new SSH host keys. Nortel recommends that you do so, in order to maintain a high level of security when connecting to the Nortel SNAS using an SSH client. If you fear that your SSH host keys have been compromised, you can create new host keys at any time by using the **`/cfg/sys/adm/sshkeys/generate`** command. When reconnecting to the Nortel SNAS after generating new host keys, your SSH client will display a warning that the host identification (or host keys) has changed.

Accessing the Nortel SNAS cluster

To enable better Nortel SNAS management and user accountability, there are five categories of users who can access the Nortel SNAS cluster:

- The Operator is granted read access only to the menus and information appropriate to this user access level. The Operator cannot make any changes to the configuration.
- The Administrator can make any changes to the Nortel SNAS configuration. Thus, the Administrator has read and write access to all menus, information, and configuration commands in the Nortel SNAS software.
- A Certificate Administrator is a member of the certadmin group. A Certificate Administrator has sufficient user rights to manage certificates and private keys. By default, only the Administrator user is a member of the certadmin group. To separate the Certificate Administrator user role from the Administrator user role, the Administrator user can add a new user account to the system, assign the new user to the certadmin group, and then remove himself or herself from the certadmin group. For more information, see “Adding a new user” (page 218).
- The Boot user can perform a reinstallation only. For security reasons, it is only possible to log on as the Boot user through the console port using terminal emulation software. The default Boot user password is `ForgetMe`. The Boot user password cannot be changed from the default.
- The Root user is granted full access to the underlying Linux operating system. For security reasons, it is only possible to log on as the Root user through the console port using terminal emulation software. Reserve Root user access for advanced troubleshooting purposes, under guidance from Nortel customer support. For more information, see “How to get help” (page 21).

Access to the Nortel SNAS CLI and settings is controlled through the use of four predefined user accounts and passwords. Once you are connected to the Nortel SNAS by a console connection or remote connection (Telnet or SSH), you are prompted to enter a user account name and the corresponding password. Table 59 "User access levels" (page 382) lists the default user accounts and passwords for each access level.

ATTENTION
The default Administrator user password can be changed during the initial configuration (see "Initial setup" (page 41)). However, the default passwords for the Operator user, the Boot user, and the Root user are used even after the initial configuration. Nortel therefore recommends that you change the default Nortel SNAS passwords for the Operator and Root user soon after the initial configuration, and as regularly as required under your network security policies.For more information about how to change a user account password, see "Changing passwords" (page 223).

Table 59
User access levels

User Account	User Group	Access Level Description	Default Password
oper	oper	The Operator is allowed read access to some of the menus and information available in the CLI.	**oper**
admin	admin oper certadmin	The Administrator is allowed both read and write access to all menus, information and configuration commands. The Administrator can add users to all groups in which the Administrator himself or herself is a member. The Administrator can delete a user from any of the other three built-in groups.	**admin**
	certadmin	By default, only the Administrator is a member of the certadmin group. Certadmin group rights are sufficient for administrating certificates and keys on the Nortel SNAS. A certificate administrator user has no access to the SSL Server menu, and only limited access to the System menu.	
boot		The boot user can only perform a reinstallation of the software, and only via a console connection.	**ForgetMe**
root		The root user has full access to the underlying Linux operating system, but only via a console connection.	**ForgetMe**

CLI Main Menu or Setup

Once the Administrator user password is verified, you are given complete access to the Nortel SNAS. If the Nortel SNAS is still set to its factory default configuration, the system will run Setup (see “Initial setup” (page 41)), a utility designed to help you through the first-time configuration process. If the Nortel SNAS has already been configured, the Main menu of the CLI is displayed instead.

Figure 22 "Administrator Main Menu" (page 383) shows the Main menu with administrator privileges.

Figure 22
Administrator Main Menu

```
[Main Menu]
      info        - Information Menu
      stats       - Statistics Menu
      cfg         - Configuration Menu
      boot        - Boot Menu
      maint       - Maintenance Menu
      diff        - Show pending config changes   [global command]
      apply       - Apply pending config changes  [global command]
      revert      - Revert pending config changes [global command]
      paste       - Restore saved config with key [global command]
      help        - Show command help menu        [global command]
      exit        - Exit [global command, always available]
```

Command line history and editing

For a description of global commands, shortcuts, and command line editing functions, see “CLI reference” (page 413).

Idle timeout

The Nortel SNAS will disconnect your local console connection or remote connection (Telnet or SSH) after 10 minutes of inactivity. This value can be changed to a maximum value of 1 hour using the **`/cfg/sys/adm/clitimeout`** command.

If you are automatically disconnected after the specified idle timeout interval, any unapplied configuration changes are lost. Therefore, make sure to save your configuration changes regularly by using the global **`apply`** command.

If you have unapplied configuration changes when you use the global **`exit`** command to log out from the CLI, you will be prompted to use the global **`diff`** command to view the pending configuration changes. After verifying the pending configuration changes, you can either apply the changes or use the **`revert`** command to remove them.

Configuration example

This chapter provides an example of a basic Nortel SNAS configuration.

This chapter includes the following topics:

Scenario

The basic Nortel SNAS network in this example includes: one Nortel SNAS device; two edge switches (one Ethernet Routing Switch 8300and one Ethernet Routing Switch 5510) functioning as network access devices ; an Ethernet Routing Switch 8600 functions only as the core router. BCM call server; a DNS server; a DHCP server; and a remediation server are connected to it. The edge switches function in Layer 2 mode.

Figure 23 "Basic configuration" (page 386) illustrates the network configuration.

Figure 23
Basic configuration

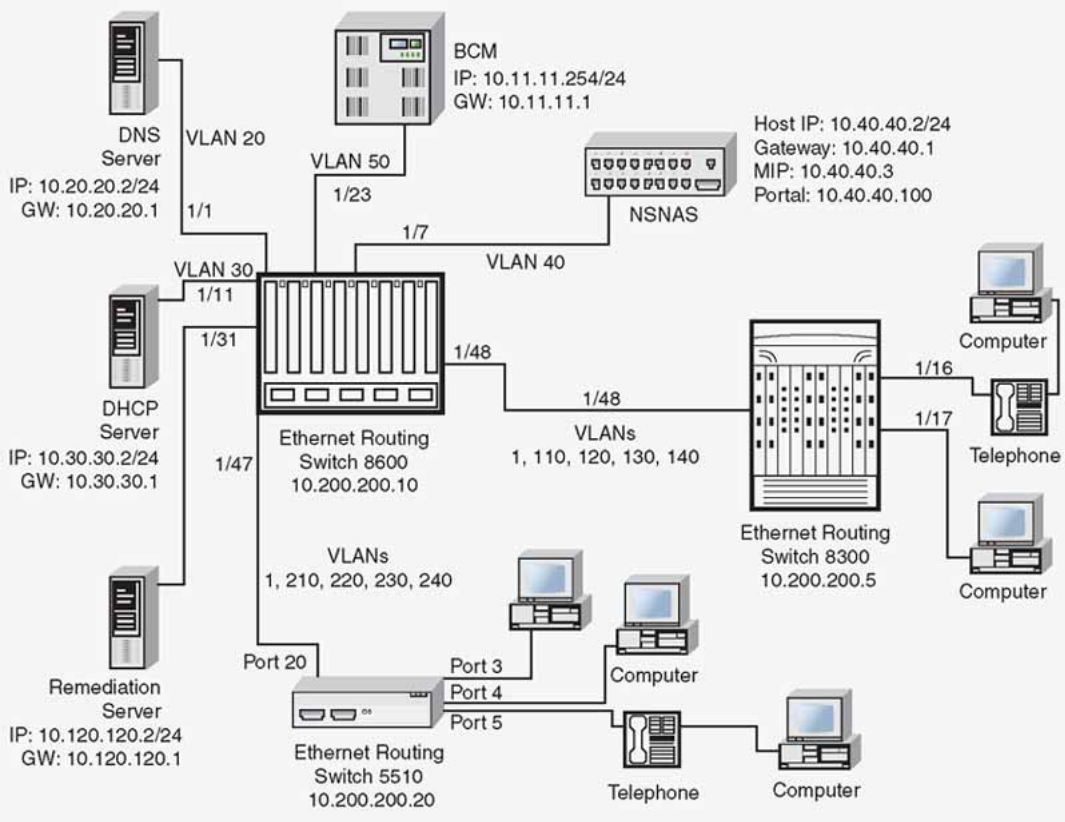


Table 60 "Network devices" (page 386) summarizes the devices connected in this environment and their respective VLAN IDs and IP addresses.

Table 60
Network devices

Device/Service	VLAN ID	VLAN IP address	Device IP address	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1 **ATTENTION** 1/1 refers to port 1 of chasis component mounted on rack 1. (1/1-- unit 1 / port 1)
DHCP	30	10.30.30.1	10.30.30.2	1/11

Table 60
Network devices (cont'd.)

Device/Service	VLAN ID	VLAN IP address	Device IP address	Ethernet Routing Switch 8600 port
Nortel SNAS	40	10.40.40.1	10.40.40.2 (RIP) 10.40.40.3 (MIP) 10.40.40.100 (pVIP)	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

Table 61 "VLANs for the Ethernet Routing Switch 8300" (page 387) summarizes the VLANs for the Ethernet Routing Switch 8300.

Table 61
VLANs for the Ethernet Routing Switch 8300

VLAN	VLAN ID	Yellow subnet
Red	110	N/A
Yellow	120	10.120.120.0/24
Green	130	N/A
VoIP	140	N/A

Table 62 "VLANs for the Ethernet Routing Switch 5510" (page 387) summarizes the VLANs for the Ethernet Routing Switch 5510.

Table 62
VLANs for the Ethernet Routing Switch 5510

VLAN	VLAN ID	Yellow subnet
Red	210	N/A
Yellow	220	10.120.120.0/24
Green	230	N/A
VoIP	240	N/A

ATTENTION
The management VLAN ID is the default (VLAN ID 1).

Steps

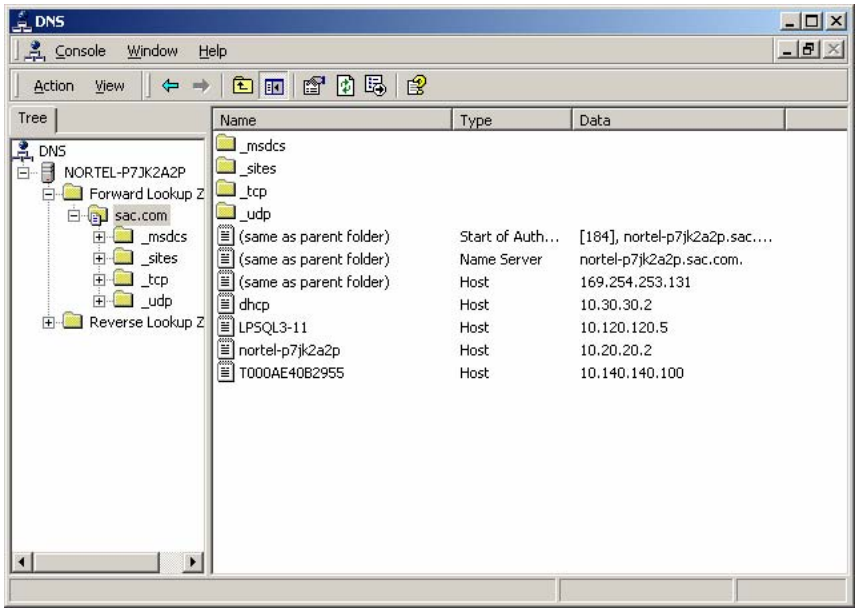
1. "Configure the network DNS server" (page 388)
2. "Configure the network DHCP server" (page 388)
3. "Configure the network core router" (page 392)
4. "Configure the Ethernet Routing Switch 8300" (page 393)

5. “Configure the Ethernet Routing Switch 5510” (page 395)
6. “Adding the network access devices ” (page 399)

Configure the network DNS server

Create a forward lookup zone for the Nortel SNAS domain (see Figure 24 "DNS Forward Lookup configuration" (page 388)). In this example, a lookup zone called sac.com has been created.

Figure 24
DNS Forward Lookup configuration

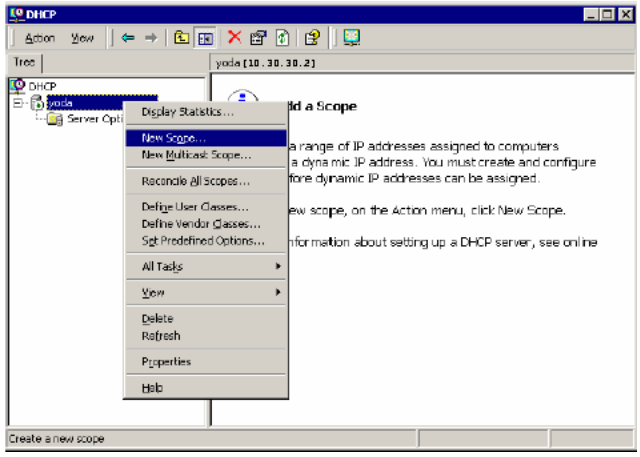


Configure the network DHCP server

To configure a DHCP scope using the New Scope Wizard (Windows 2000 server):

Step	Action
1	Log in to the server using the administrator username and password.
2	Run the DHCP admin utility (Start **> Programs > Administrative Tools > DHCP**).
3	Create a new DHCP scope (see Figure 25 "Creating a new DHCP scope" (page 389)).

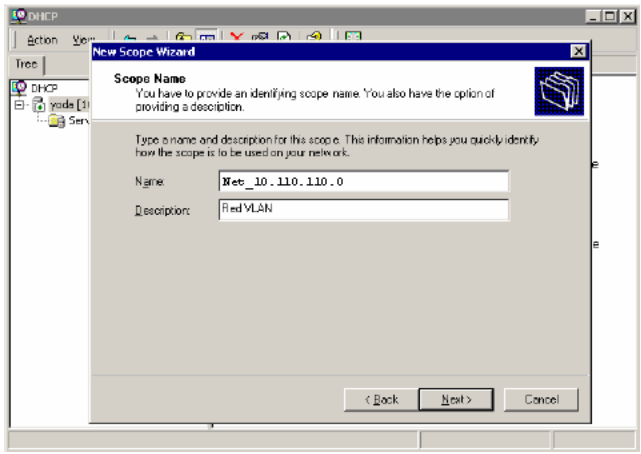
Figure 25
Creating a new DHCP scope



4 Enter a descriptive name to identify the new scope (see Figure 26 "Naming the new DHCP scope" (page 389)).

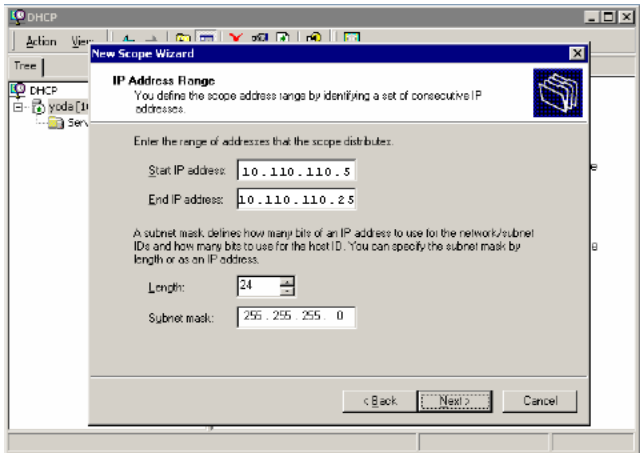
In this example, you are creating a DHCP scope for the Red VLAN on the Ethernet Routing Switch 8300. The scope start address for the VLAN is 10.110.110.5 and the end address is 10.110.110.25. The scope you create must have a range of IP addresses that is large enough to accommodate all endpoint devices in your network.

Figure 26
Naming the new DHCP scope



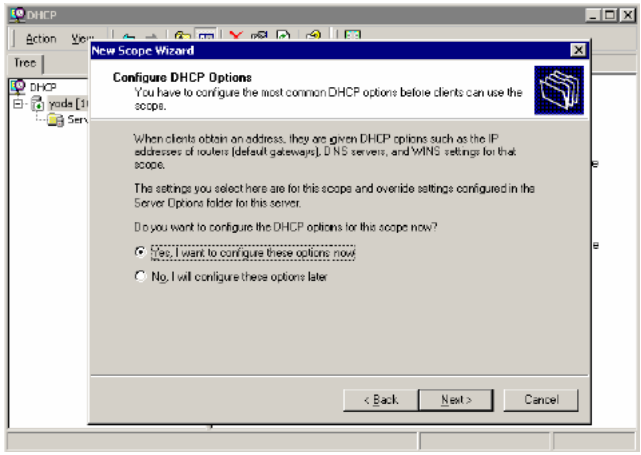
5 Specify the IP address range for the DHCP scope (see Figure 27 "Specifying the IP address range" (page 390)).

Figure 27
Specifying the IP address range



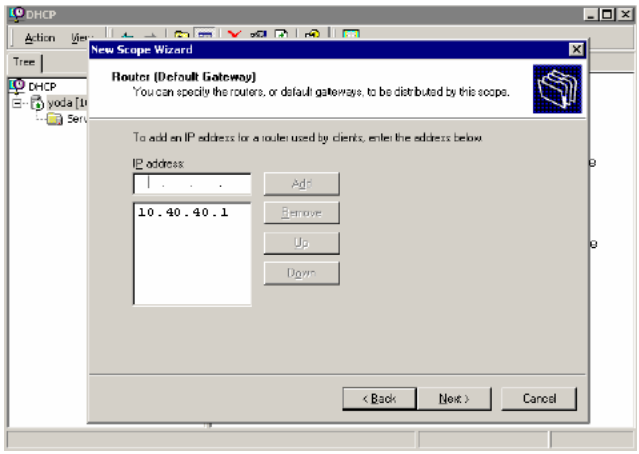
6 Select the **Yes, I want to configure these options now** option button on the **Configure DHCP Options** window (see Figure 28 "Choosing to configure additional options" (page 390)).

Figure 28
Choosing to configure additional options



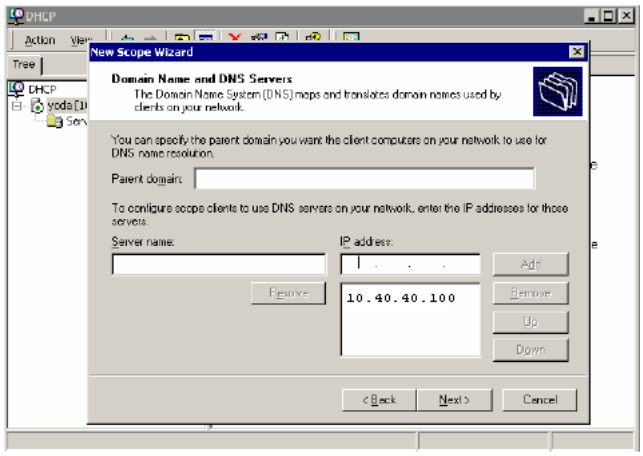
7 Enter the IP address of the default gateway (see Figure 29 "Specifying the default gateway" (page 391)).

Figure 29
Specifying the default gateway



8 Enter the IP address of the DNS server (see Figure 30 "Specifying the DNS server" (page 391)).

Figure 30
Specifying the DNS server

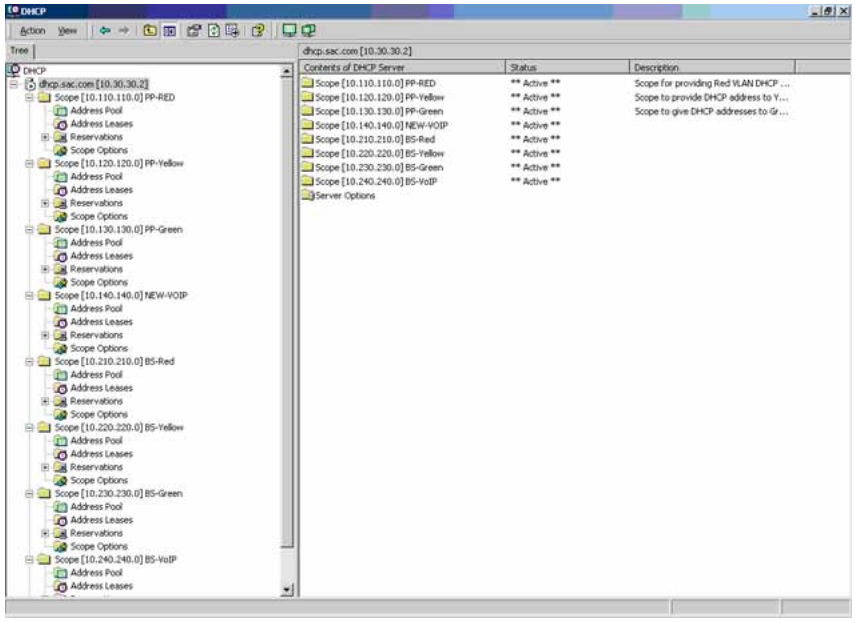


ATTENTION
In this configuration example, the Nortel SNAS will function as a captive portal. For the Red VLAN scope, the DNS server must be the Nortel SNAS portal Virtual IP address (pVIP). For the Yellow and Green VLAN scopes, enter the IP addresses for the regular DNS servers in your network.

9 Repeat step 3 through step 8 for each Red, Yellow, and Green VLAN in the network.

Figure 31 "After all DHCP scopes have been created" (page 392) shows the DHCP scopes created for use in this example.

Figure 31
After all DHCP scopes have been created



--End--

Configure the network core router

There are no special requirements for the core router in a Nortel SNAS network. Refer to the regular documentation for the type of router used in your network.

Step	Action
1	Create the Red, Yellow, Green, VoIP, and Nortel SNAS management VLANs.
2	Assign the VLAN port members. Since the edge switches in this example are operating in Layer 2 mode, enable 802.1q tagging on the uplink ports to enable them to participate in multiple VLANs, then add the ports to the applicable VLANs.
3	Create IP interfaces for the VLANs.
4	Since the edge switches are operating in Layer 2 mode, configure DHCP relay agents for the Red, Yellow, Green, and VoIP VLANs.

Use the applicable show commands on the router to verify that DHCP relay has been activated to reach the correct scope for each VLAN.

--End--

Configure the Ethernet Routing Switch 8300

The configuration procedure is based on the following assumptions:

- You are starting with an installed switch that is not currently configured as part of the network.
- You have installed Software Release 2.2.8.
- You have configured basic switch connectivity.
- You have initialized the switch and it is ready to accept configuration.
- You have configured devices as described to this point.

Steps

To configure the Ethernet Routing Switch 8300for the Nortel SNAS network, perform the following steps:

1. “Enabling SSH” (page 393)
2. “Configuring the Nortel SNAS pVIP subnet” (page 394)
3. “Creating port-based VLANs” (page 394)
4. “Configuring the VoIP VLANs” (page 394)
5. “Configuring the Red, Yellow, and Green VLANs” (page 394)
6. “Configuring the NSNA uplink filter” (page 394)
7. “Configuring the NSNA ports” (page 394)
8. “Enabling NSNA globally” (page 395)

Enabling SSH

```
Passport-8310:5# config bootconfig flags ssh true
Passport-8310:5# config sys set ssh enable true
Passport-8310:5# config load-module 3DES /flash/P83C2280.
IMG
```

ATTENTION
You have the option of using the AES encryption module, instead of the 3DES module.

Configuring the Nortel SNAS pVIP subnet

```
Passport-8310:5# config nsna nsnas 10.40.40.0/24 add
```

Creating port-based VLANs

```
Passport-8310:5# config vlan 110 create byport 1
Passport-8310:5# config vlan 120 create byport 1
Passport-8310:5# config vlan 130 create byport 1
Passport-8310:5# config vlan 140 create byport 1
```

Configuring the VoIP VLANs

```
Passport-8310:5# config vlan 140 nsna color voip
```

Configuring the Red, Yellow, and Green VLANs

```
Passport-8310:5# config vlan 110 nsna color red filter-id
310
Passport-8310:5# config vlan 120 nsna color yellow
filter-id 320 yellow-subnet-ip 10.120.120.0/24
Passport-8310:5# config vlan 130 nsna color green filter-id
330
```

Configuring the NSNA uplink filter

```
Passport-8310:6# config filter acl 100 create ip acl-name
"dhcp"
Passport-8310:6/config#
filter acl 100 ace 1 create
Passport-8310:6# config filter acl 100 ace 1 action fwd2cpu
precedence 1
Passport-8310:6# config filter acl 100 ace 1 ip ipfragment
non-fragments
Passport-8310:6# config filter acl 100 ace 1 protocol udp eq
any
Passport-8310:6# config filter acl 100 ace 1 port dst-port
bootpd-dhcp
Passport-8310:6# config filter acl 100 ace default action
permit
Passport-8310:6# config filter acg 100 create 100 acg-name
"uplink"

Passport-8310:6# config ethernet <slot/port> filter create
100
```

Configuring the NSNA ports

Add the uplink port:

```
Passport-8310:6# config ethernet 1/48 nsna uplink
uplink-vlans 110,120,130,140
```

Add the client ports:

```
Passport-8310:5# config ethernet 1/16-1/17 nsna dynamic
```

Enabling NSNA globally

```
Passport-8310:5# config nsna state enable
```

Configure the Ethernet Routing Switch 5510

The following configuration example is based on the following assumptions:

- You are starting with an installed switch that is not currently configured as part of the network.
- You have installed Software Release 4.3.
- You have configured basic switch connectivity.
- You have initialized the switch and it is ready to accept configuration.
- You have configured devices as described to this point.

Steps

To configure the Ethernet Routing Switch 5510 for the Nortel SNAS network, perform the following steps:

1. “Setting the switch IP address” (page 395)
2. “Configuring SSH” (page 395)
3. “Configuring the Nortel SNAS pVIP subnet” (page 394)
4. “Creating port-based VLANs” (page 396)
5. “Configuring the VoIP VLANs” (page 396)
6. “Configuring the Red, Yellow, and Green VLANs” (page 396)
7. “Configuring the login domain controller filters” (page 396)
8. “Configuring the NSNA ports” (page 396)
9. “Enabling NSNA globally” (page 397)

Setting the switch IP address

```
5510-48T(config)# ip address 10.200.200.20 netmask
255.255.255.0
5510-48T(config)# ip default-gateway 10.200.200.10
```

Configuring SSH

In this example, the assumption is that the Nortel SNAS public key has already been uploaded to the TFTP server (10.20.20.20).

```
5510-48T(config)# ssh download-auth-key address
10.20.20.20 key-name sac_key.1.pub

5510-48T(config)# ssh
```

Configuring the Nortel SNAS pVIP subnet

```
5510-48T(config)# nsna nsnas 10.40.40.0/24
```

Creating port-based VLANs

```
5510-48T(config)# vlan create 210 type port
5510-48T(config)# vlan create 220 type port
5510-48T(config)# vlan create 230 type port
5510-48T(config)# vlan create 240 type port
```

Configuring the VoIP VLANs

```
5510-48T(config)# nsna vlan 240 color voip
```

Configuring the Red, Yellow, and Green VLANs

```
5510-48T(config)# nsna vlan 210 color red filter red

5510-48T(config)# nsna vlan 220 color yellow filter yellow
yellow-subnet 10.120.120.0/24

5510-48T(config)# nsna vlan 230 color green filter green
```

Configuring the login domain controller filters

ATTENTION
This step is optional.

The PC client must be able to access the login domain controller you configure (that is, clients using the login domain controller must be able to ping that controller).

```
5510-48T(config)# qos nsna classifier name RED dst-ip
10.200.2.12/32 ethertype 0x0800 drop-action disable block
wins-prim-sec eval-order 70

5510-48T(config)# qos nsna classifier name RED dst-ip
10.200.224.184/32 ethertype 0x0800 drop-action disable
block wins-prim-sec eval-order 71
```

Configuring the NSNA ports

Add the uplink port:

```
5510-48T(config)# interface fastEthernet 20
5510-48T(config-if)# nsna uplink vlans 210,220,230,240
5510-48T(config-if)# exit
```

Add the client ports:

```
5510-48T(config)# interface fastEthernet 3-5
5510-48T(config-if)# nsna dynamic voip-vlans 240
5510-48T(config-if)# exit
```

Enabling NSNA globally

```
5510-48T(config)# nsna enable
```

Configure the Nortel SNAS

To configure the Nortel SNAS, perform the following steps:

1. “Performing initial setup” (page 397)
2. “Completing initial setup” (page 398)
3. “Adding the network access devices ” (page 399)
4. “Mapping the VLANs” (page 401)
5. “Enabling the network access devices ” (page 401)

Performing initial setup

Establish a serial console connection to the Nortel SNAS device. The Setup utility launches automatically on startup.

```
Alteon iSD NSNAS
Hardware platform:  4050
Software version:  x.x
-------------------------------------------------------
[Setup Menu]
   join    - Join an existing cluster
   new   - Initialize host as a new installation
   boot   - Boot menu
   info    - Information menu
   exit    - Exit [global command, always available]

>> Setup# new

Setup will guide you through the initial configuration.

Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management
interface): 10.40.40.2
Enter network mask [255.255.255.0]:  <mask>
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (or blank to skip):
10.40.40.1
Enter the Management IP (MIP) address: 10.40.40.3
```

```
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
Enter a timezone or 'select' [select]: America/Los_Angeles
Enter the current date (YYYY-MM-DD) [2005-05-02]:
Enter the current time (HH:MM:SS) [19:14:52]:
Enter NTP server address (or blank to skip):
Enter DNS server address (or blank to skip): 10.20.20.2
Generate new SSH host keys (yes/no) [yes]:
This may take a few seconds...ok
Enter a password for the "admin" user:
Re-enter to confirm:
Run NSNAS quick setup wizard [yes]:
   Creating default networks under /cfg/doamin #/aaa/
   network
Enter NSNAS Portal Virtual IP address(pvip): 10.40.40.100
Enter NSNAS Domain name: Domain1
Enter comma separated DNS search list
(eg company.com,intranet.company.com):
Create http to https redirect server [no]:
Use restricted (teardown/restricted) action for Nortel
Health Agent failure?  [yes]:
Create default tunnel guard user [no]: yes
Using 'restricted' action for Nortel Health Agent failure.
User name:  nha
User password:  nha
   Creating client filter 'nha_passed'.
   Creating client filter 'nha_failed'.
   Creating linkset 'nha_passed'.
   Creating linkset 'nha_failed'.
   Creating group 'nhauser' with secure access.
   Creating extended profile, full access when nha_passed
Enter green vlan id [110]: 130
   Creating extended profile, remediation access when
nha_failed
Enter yellow vlan id [120]:
   Creating user 'nha' in group 'nhauser'.
Initializing system......ok
Setup successful.  Relogin to configure.
```

Completing initial setup

Enable SSH for secure management communications (required for SREM):

```
>> Main# cfg/sys/adm/ssh on
```

Enable SRS administration:

```
>> Main# cfg/sys/adm/srsadmin/ena
```

Generate and activate the SSH key for communication with the network access devices:

```
>> Main# cfg/doamin #/sshkey/generate
Generating new SSH key, this operation takes a few
seconds...  done.
Apply to activate.

>> NSNAS SSH key# apply
```

Create a test SRS rule and specify it for the nhauser group:

```
>> Group 1# /cfg/doamin #/aaa/nha/quick
In the event that the Nortel Health Agent checks fails on a
client,
the session can be teardown, or left in restricted mode
with limited access.
Which action do you want to use for Nortel Health Agent
failure?  (teardown/restricted) [restricted]:
Do you want to create a Nortel Health Agent test user?
(yes/no)
[yes]: no
Using existing nha_passed filter
Using existing nha_failed filter
Using existing nha_passed linkset
Using existing nha_failed linkset
Adding test SRS rule srs-rule-test
This rule check for the presence of the file
C:\tunnelguard\tg.txt
Using existing nha_passed filter

Use 'diff' to view pending changes, and 'apply' to commit

>> NHA# ../group #/srs srs-rule-test
>> Group 1# apply
```

Adding the network access devices

This example adds the Ethernet Routing Switch 8300manually, and uses the quick switch wizard to add the Ethernet Routing Switch 5510. In both cases, the example assumes that the switch is not reachable when it is added, and the switch public SSH key is therefore not automatically retrieved by the Nortel SNAS.

Adding the Ethernet Routing Switch 8300 Add the switch manually:

```
>> Main# cfg/doamin #/switch 1
Creating Switch 1
Enter name of the switch: Switch1_ERS8300
Enter the type of the switch (ERS8300/ERS5500): ERS8300
Enter IP address of the switch: 10.200.200.5
NSNA communication port [5000]:
Enter VLAN Id of the Red VLAN: 110
Entering:  SSH Key menu
Enter username: rwa
Leaving:  SSH Key menu

------------------------------------------------------------
-----
[Switch 1 Menu]
   name   - Set Switch name
   type    - Set Type of the switch
   ip      - Set IP address
   port    - Set NSNA communication port
   hlthchk  - Health check intervals for switch
   vlan    - Vlan menu
   rvid    - Set Red VLAN Id
   sshkey  - SSH Key menu
   reset    - Reset all the ports on a switch
   ena     - Enable switch
   dis     - Disable switch
   delete   - Remove Switch
Error:  Failed to retrieve host key

>> Switch 1# apply
Changes applied successfully.
```

Export the Nortel SNAS public SSH key to the Ethernet Routing Switch 8300:

```
>> Switch 1# sshkey/export
```

Import the public SSH key from the switch:

```
>> SSH Key# import
```

Adding the Ethernet Routing Switch 5510 Use the quick switch wizard:

```
>> Main# cfg/doamin #/quick
Enter the type of the switch (ERS8300/ERS5500) [ERS8300]:
ERS55
IP address of Switch: 10.200.200.20
NSNA communication port [5000]:
```

```
Trying to retrieve fingerprint...failed.
Error:  "Failed to retrieve host key"
Do you want to add ssh key?  (yes/no) [no]:
Red vlan id of Switch: 210
Creating Switch 2
Use apply to activate the new Switch.

>> doamin ##
```

Export the Nortel SNAS public SSH key to a TFTP server, for manual retrieval by the Ethernet Routing Switch 5500:

```
>> Main# cfg/doamin #/sshkey/export tftp 10.20.20.20
sac_key.1.pub
```

Import the public SSH key from the switch:

```
>> Main# cfg/doamin #/switch 2/sshkey/import
```

Mapping the VLANs

This example assumes that the VLANs defined on the Ethernet Routing Switch 8300(Switch 1) will always be used exclusively by Switch 1, whereas the VLAN IDs for the VLANs defined on the Ethernet Routing Switch 5510 (Switch 2) may be used by other edge switches added to the domain in future. Therefore, the VLAN mappings for Switch 1 are made at the switch-level command, while the VLAN mappings for Switch 2 are made at the domain level.

```
>> Main# cfg/doamin #/switch 1/vlan/add yellow 120
>> Switch Vlan# add green 130
>> Switch Vlan# ../../vlan/add yellow 220
>> Domain Vlan# add green 230
>> Domain Vlan# apply
Changes applied successfully.
```

Enabling the network access devices

```
>> Main# cfg/doamin #/switch 1/ena
>> Switch 1# ../switch 2/ena
>> Switch 2# apply
Changes applied successfully.
```

Troubleshooting

This chapter includes the following topics:

Troubleshooting tips

This chapter provides troubleshooting tips for the following problems:

Cannot connect to the Nortel SNAS using Telnet or SSH

Verify the current configuration

Connect with a console connection and check that Telnet or SSH access to the Nortel SNAS is enabled. By default, remote connections to the Nortel SNAS are disabled for security reasons. Enter the command **`/cfg/sys/adm/cur`** to see whether remote access is enabled for Telnet or SSH.

```
>> Main# /cfg/sys/adm/cur

Administrative Applications:
  SONMP Protocol participation = off
  CLI idle timeout = 10m
  Telnet CLI access = on
  SSH CLI access = off

    SNMP:
      Enable SNMP = true
      SNMP versions supported = v1,v2c,v3

        SNMPv2-MIB:
          SysContact =
          SnmpEnableAuthenTraps = disabled

        SNMP Community:
          Read Community String = public
          Write Community String =
          Trap Community String = trap

    Audit:
      Vendor id for audit attribute = 1872 (alteon)
      Vendor type for audit attribute = 2
      Enable Audit = false
Press q to quit, any other key to continue
```

Enable Telnet or SSH access

If your security policy affords enabling remote connections to the Nortel SNAS, enter the command **/cfg/sys/adm/telnet** to enable Telnet access, or the command **/cfg/sys/adm/ssh** to enable SSH access. Apply your configuration changes.

```
>> Main# /cfg/sys/adm/ssh
Current value:  off
Allow SSH CLI access (on/off): on
>> Administrative Applications# apply
Changes applied successfully.
```

Check the Access List

If you find that Telnet or SSH access is enabled but you still cannot connect to the Nortel SNAS using a Telnet or SSH client, check whether any hosts have been added to the Access List. Enter the command **/cfg/sys/accesslist/list** to view the current Access List.

```
>> Main# /cfg/sys/accesslist/list
  1:  192.168.128.78, 255.255.255.0
```

When Telnet or SSH access is enabled, only those hosts listed in the Access List are allowed to access the Nortel SNAS over the network. If no hosts have been added to the Access List, this means that any host is allowed to access the Nortel SNAS over the network (assuming that Telnet or SSH access is enabled).

If there are entries in the Access List but your host is not listed, use the **/cfg/sys/accesslist/add** command to add the required host to the Access List.

Check the IP address configuration

If your host is allowed to access the Nortel SNAS over the network according to the Access List, check that you have configured the correct IP addresses on the Nortel SNAS.

Ensure that you ping the host IP address (RIP) of the Nortel SNAS, and not the Management IP address (MIP) of the cluster in which the Nortel SNAS is a member. Enter the command **/cfg/cur sys** to view IP address information for all Nortel SNAS devices in the cluster.

```
>> Main# /cfg/cur sys

System:
  Management IP (MIP) address = 172.16.120.50

    Cluster Host 1:
      IP address = 172.16.120.51
      SysName =
      SysLocation =
      License =
        NSNAS sessions: 200
      Default gateway address = 172.16.120.1
      Ports = 1,2,3
      Hardware platform = 4070

        Host Routes:
          No items configured

        Host Interface 1:
          IP address = 172.16.120.51
          Network mask = 255.255.255.0
          Default gateway address = 0.0.0.0
          VLAN tag id = 0
          Mode = failover
          Primary port = 0
Press q to quit, any other key to continue_
```

If the IP address assigned to the Nortel SNAS is correct, you may have a routing problem. Try to run **traceroute** (a global command available at any menu prompt) or the **tcpdump** command (or some other network analysis tool) to locate the problem. For more information about the **tcpdump** command, see "Tracing SSL traffic" (page 99).

If this does not help you to solve the problem, contact Nortel for technical support. See "How to get help" (page 21).

Cannot add the Nortel SNAS to a cluster

When you try to add a Nortel SNAS device to a cluster by selecting **join** in the Setup menu, you may receive an error message stating that the system is running an incompatible software version.

The incompatible software version referred to in the error message is the software that is running on the Nortel SNAS device you are trying to add to the cluster. This error message is displayed whenever the Nortel SNAS you are trying to add has a different software version from the Nortel SNAS device already in the cluster. In this situation, do one of the following:

- Adjust the software version on the Nortel SNAS device you are trying to add to the cluster, to synchronize it with the software version running on the Nortel SNAS device already in the cluster. You can verify

software versions by typing the command **/boot/software/cur**. The active software version is indicated as `permanent`.
To adjust the software version on the Nortel SNAS device you want to add to the cluster, you must either upgrade to a newer software version or revert to an older software version. In either case, perform the steps described in "Reinstalling the software" (page 372). After you adjust the software version, log on as the Administrator user and select **join** from the Setup menu.

- Upgrade the software version running on the Nortel SNAS device in the cluster to the same version as running on the Nortel SNAS you want to add to the cluster. Perform the steps described in "Performing minor and major release upgrades" (page 368). Then add the Nortel SNAS device by selecting **join** from the Setup menu.

Cannot contact the MIP

When you try to add a Nortel SNAS to a cluster by selecting **join** in the Setup menu, you may receive an error message stating that the system is unable to contact the Management IP address (MIP).

The problem may be that there are existing entries in the Access List. When Telnet or SSH access is enabled, only those hosts listed in the Access List are allowed to access the Nortel SNAS over the network. If no hosts have been added to the Access List, this means that any host is allowed to access the Nortel SNAS over the network (assuming that Telnet or SSH access is enabled).

If the Access List contains entries, add the Interface 1 IP addresses of both Nortel SNAS devices as well as the MIP to the Access List before you attempt the join.

Check the Access List

On the existing Nortel SNAS device in the cluster, check whether any hosts have been added to the Access List. Enter the command **/cfg/sys/accesslist/list** to view the current Access List.

```
>> Main# /cfg/sys/accesslist/list
  1:  192.168.128.78, 255.255.255.0
```

Add Interface 1 IP addresses and the MIP to the Access List

Use the **/cfg/cur sys** command to view the Host Interface 1 IP address for the existing Nortel SNAS. Then use the **/cfg/sys/accesslist/add** command to add this IP address, the Interface 1 IP address you intend to use for the new Nortel SNAS, and the MIP to the Access List.

```
>> Main# /cfg/sys/accesslist/add
Enter network address: <IP address>
Enter netmask: <network mask>
```

Try again to add the Nortel SNAS to the cluster using the **join** command in the Setup menu.

The Nortel SNAS stops responding

Telnet or SSH connection to the MIP

When you are connected to a cluster of Nortel SNAS devices through a Telnet or SSH connection to the MIP, your connection to the cluster can be maintained as long as at least one Nortel SNAS device in the cluster is up and running. However, if the particular Nortel SNAS that currently is in control of the MIP stops responding while you are connected, you must close down your Telnet or SSH connection and reconnect to the MIP.

After you reconnect, use the **/info/contlist** command to view the operational status of all Nortel SNAS devices in the cluster. If the operational status of one of the Nortel SNAS devices is indicated as down, reboot that machine: On the Nortel SNAS device, press the Power button on the back panel to turn the machine off, wait until the fan comes to a standstill, and then press the Power button again to turn the machine on.

Log on as the Administrator user when the logon prompt appears and check the operational status again.

Console connection

If you are connected to a particular Nortel SNAS device through a console connection and the device stops responding, press the key combination **Ctrl+^**, then press **Enter**. This takes you back to the login prompt. Log on as the Administrator user and check the operational status of the Nortel SNAS. Enter the command **/info/contlist** to view the operational status of the device.

If the operational status of the Nortel SNAS is indicated as down, try rebooting the device by typing the command **/boot/reboot**. You will be asked to confirm your action before the actual reboot is performed. Log on as the Administrator user and again use the **/info/contlist** command to check if the operational status of the Nortel SNAS is now up.

If the operational status of the Nortel SNAS is still down, reboot the machine. On the device, press the Power button on the back panel to turn the machine off, wait until the fan comes to a standstill, and then press the Power button again to turn the machine on. Log on as the Administrator user when the login prompt appears.

A user password is lost

There are four types of system user passwords:

- “Administrator user password” (page 408)
- “Operator user password” (page 408)
- “Root user password” (page 408)
- “Boot user password” (page 408)

Administrator user password

If you have lost the Administrator user password the only way to regain access to the Nortel SNAS as the Administrator user is to reinstall the software, using a console connection as the Boot user.

For more information, see “Reinstalling the software” (page 372).

Operator user password

If you have lost the Operator user password, log on as the Administrator user and define a new Operator user password. Only the Administrator user can change the Operator user password.

For more information, see “*Changing another users password*” (page 224) .

Root user password

If you have lost the Root user password, log on as the Administrator user and define a new Root user password. Only the Administrator user can change the Root user password. For more information, see “*Changing another users password*” (page 224) .

Boot user password

The default Boot user password cannot be changed, and can therefore never really be lost. If you have forgotten the Boot user password, see “Accessing the Nortel SNAS cluster” (page 381).

The reason the Boot user password cannot be changed is that, if you lost both the Administrator password and the Boot user password, the Nortel SNAS would be rendered completely inaccessible to all users except the Operator, who does not have rights to make configuration changes.

The fact that the Boot user password cannot be changed is not a security concern. The Boot user can only access the Nortel SNAS with a console connection using a serial cable, and it is assumed that the Nortel SNAS device is set up in a server room with restricted access.

A user fails to connect to the Nortel SNAS domain

The following are common reasons why a user may have difficulty authenticating to the Nortel SNAS domain or why a client connection cannot be established.

- The user name or password is wrong.
- The configured authentication server cannot be reached.
- The group name retrieved from the authentication server does not exist on the Nortel SNAS.

Trace tools

Use the **/maint/starttrace** command to trace the different steps involved in a specific process, such as authorization.

```
>> Main# maint/starttrace
Enter tags (list of all,aaa,dhcp,dns,ssl,tg,snas,patchlink,ra
dius,nap) [all]: aaa,ssl
Enter Domain (or 0 for all Domains) [0]:
Output mode (interactive/tftp/ftp/sftp) [interactive]:
```

For more information about the **starttrace** command, the tags you can specify for the trace, and the available output modes, see "Performing maintenance" (page 353).

Table 63 "Sample output for the trace command" (page 409) shows sample output for the various tags.

Table 63
Sample output for the trace command

Tag	Description	Sample output
aaa	Logs authentication method, user name, group, and profile	>> Maintenance# 12:54:08.875111: Trace started 12:54:28.834571 10.1.82.145 (1) aaa: "local user db Accept 1:john with groups ["trusted"]" 12:54:28.835144 10.1.82.145 (1) aaa: "final groups for user: john groups: trusted:<base> " 12:54:29.917926 10.1.82.145 (1) aaa: "new groups for user: john groups: trusted:<base> "
dns	Logs failed DNS lookups made during a session	>> Maintenance# 13:00:09.868682 10.1.82.145 (1) dns: "Failed to lookup www.example.com in DNS (DNS domain name does not exist)"

Table 63
Sample output for the trace command (cont'd.)

Tag	Description	Sample output
ssl	Logs information related to the SSL handshake procedure (for example, the cipher used)	>> Maintenance# 13:15:55.985432: Trace started 13:16:26.808831 10.1.82.145 (1) ssl: "SSL accept done, cipher is RC4-MD5" 13:16:28.802199 10.1.82.145 (1) ssl: "SSL accept done, cipher is RC4-MD5" 13:16:29.012856 10.1.82.145 (1) ssl: "SSL accept done, cipher is RC4-MD5"
nha	Logs information related to a Nortel Health Agent check (for example, SRS rule check result)	>> Maintenance# 13:27:50.715545: Trace started 13:27:54.976137 10.1.82.145 (1) nha: "ssl user john[192.168.128.19] - starting Nortel Health Agent ssl session" 13:28:17.204049 10.1.82.145 (1) nha: "ssl user john[192.168.128.19] - agent authentication ok" 13:28:18.807447 10.1.82.145 (1) nha: "user john[192.168.128.19] - SRS checks ok, open session"

To disable tracing, press **Enter** to display the Maintenance menu prompt, then enter **`stoptrace`**.

System diagnostics

The following are useful diagnostic display commands. For more information about the commands, use the alphabetical listings in "CLI reference" (page 413) to cross-reference to where the commands are described in more detail in this guide.

Installed certificates

To view the currently installed certificates, enter the following command:

```
>> Main# /info/certs
```

To view detailed information about a specific certificate, access the Certificate menu and specify the desired certificate by its index number:

```
>> Main# /cfg/cert
Enter certificate number: (1-) <certificate number by index>
>> Certificate 1# show
```

Network diagnostics

To check if the Nortel SNAS is able to contact configured network access devices, routers, DNS servers, authentication servers, and IP addresses or domain names specified in group links, use the following command:

```
>> Main# /maint/chkcfg
```

The screen output provides information about each configured network element and shows whether the network test was successful or not. The method used to check the connection (for example, ping) is also displayed.

To check network settings for a specific Nortel SNAS, access the Cluster Host menu by typing the following commands:

```
>> Main# /cfg/sys/host <host by index number>
>> Cluster Host 1# cur
```

To check general network settings related to the cluster to which you have connected, enter the following command:

```
>> Main# /cfg/sys/cur
```

The screen output provides information about the MIP, DNS servers, Nortel SNAS hosts in the cluster, syslog servers, and NTP servers.

To check if the Nortel SNAS is getting network traffic, enter the following command:

```
>> Main# /stats/dump
```

The screen output provides information about currently active request sessions, total completed request sessions, and SSL statistics for configured virtual SSL servers.

To check statistics for the local Ethernet network interface card, enter the following command:

```
>> Main# /info/ethernet
```

The screen output provides information about the total number of received and transmitted packets, the number of errors when receiving and transmitting packets, and the type of error (such as dropped packets, overrun packets, malformed packets, packet collisions, and lack of carrier).

To check if a virtual server (on the Nortel SNAS) is working, enter the following command at any menu prompt:

```
>> Main# ping <IP address of virtual server>
```

To capture and analyze TCP traffic between clients and the virtual SSL server, enter the following command:

```
>> Main# /cfg/doamin #/server/trace/tcpdump
```

To capture and analyze decrypted SSL traffic sent between clients and the portal server, enter the following command:

```
>> Main# /cfg/doamin #/server/trace/ssldump
```

Active alarms and the events log file

To view an alarm that has been triggered and is active, enter the following command:

```
>> Main# /info/events/alarms
```

To save the events log file to an FTP/TFTP/SFTP server, enter the following command:

```
>> Main# /info/events/download
```

You must provide the IP address or host name of the FTP/TFTP/SFTP server, as well as a file name. After the events log file has been saved, connect to the FTP/TFTP/SFTP server and examine the contents of the file.

Error log files

If you have configured the Nortel SNAS to use a syslog server, the Nortel SNAS sends log messages to the specified syslog server. For information about configuring a UNIX Syslog daemon, see the Syslog manpages under UNIX. For information about configuring the Nortel SNAS to use a syslog server, see “Configuring syslog servers” (page 279).

You can also use the **/maint/dumplogs** command. The command collects system log file information from the Nortel SNAS to which you are connected (or, optionally, all Nortel SNAS devices in the cluster) and sends the information to a file in the gzip compressed tar format on the TFTP/FTP/SFTP server you specify. The information can then be used for technical support purposes. The file sent to the TFTP/FTP/SFTP server does not contain any sensitive information related to the system configuration, such as certificates or private keys.

Appendix CLI reference

The command line interface (CLI) allows you to view system information and statistics. The Administrator can use the CLI for configuring the Nortel SNAS system, software, and individual devices in the system.

This appendix includes the following topics:

Using the CLI

CLI commands are grouped into a series of menus and submenus (see “CLI Main Menu” (page 421)). Each menu contains a list of available commands and a summary of each command function.

You can enter menu commands at the prompt that follows each menu.

Global commands

Basic commands are recognized throughout the menu hierarchy. Use the global commands in Table 64 "Global commands" (page 414) to obtain online help, navigate through menus, and apply and save configuration changes.

Table 64
Global commands

Command	Action
`help`	Display a summary of the global commands.
`help <command>`	Display help on a specific command in the command line interface.
`.`	Display the current menu.
`print`	Display the current menu.
`..`	Advance one level in the menu structure.
`up`	Advance one level in the menu structure.
`/`	Placed at the beginning of a command, returns to the Main menu. Placed within a command string, the character separates multiple commands on the same line.
`cd "<menu/path>"`	Display the menu indicated within quotation marks. **TIP:** Type `cd "/cfg/sys"` at any prompt in the CLI to go to the System menu. Also type `/cfg/sys` (no quotation marks) at any menu prompt to go to the System menu.
`pwd`	Display the command path used to reach the current menu.
`apply`	Apply pending configuration changes.
`diff`	Show any pending configuration changes.
`revert`	Remove pending configuration changes between `apply` commands. **TIP:** Use `revert` to restore configuration parameters set after the most recent apply command.
`paste`	Restores a saved configuration that includes private keys. **TIP:** Before you paste the configuration, you must provide the password phrase you specified when you selected *include the private keys in the configuration dump*. For more information, see the `dump` command in "Configuration menu" (page 424).
`exit`	Terminate the current session and log out. **TIP:** You are notified if there are unapplied (pending) configuration changes when you execute the `exit` command. Pending configuration changes are lost if you log out without executing the apply command.
`quit`	Terminate the current session and log out. **TIP:** You are notified if there are unapplied (pending) configuration changes when you execute the `quit` command,. Pending configuration chagnes are lost if you log out without executing the apply command.

Table 64
Global commands (cont'd.)

Command	Action
Ctrl+^	Exit from the command line interface if the Nortel Secure Network Access Switch has stopped responding. **TIP:** This command should be used only when you are connected to a specific Nortel Secure Network Access Switch through a console connection. Do not use this command when connected to the Management IP of the cluster through a Telnet or SSH connection.
netstat	Show the current network status of the Nortel Secure Network Access Switch. The **netstat** command provides information about active TCP connections, the state of all TCP/IP servers, and the sockets the servers use.
nslookup	Find the IP address or host name of a machine. **TIP:** To use the **nslookup** command, the Nortel Secure Network Access Switch must be configured to use a DNS server.
ping <IPaddr or host name>	Verify station-to-station connectivity across the network. **TIP:** You can specify an IP address or host name in the command. To specify host names, you must configure the DNS parameters.
traceroute <IPaddr or host name>	Identify the route used for station-to-station connectivity across the network. **TIP:** You can specify an IP address or host name of the target station in the command. To specify host names, you must configure the DNS parameters.
cur	View all the current settings for the active menu. The global command cur can be executed with arguments **cur [<path>] [<depth>]** .
curb	Obtain a summary of the current settings for the active menu. The global command curb cab be executed with arguments **curb [<path>] [<depth>]** .
dump	Dump the current configuration for the active menu. **TIP:** You can cut and paste the dumped information into the CLI of another operator at the same menu level. In all Statistics menus, the dump command provides statistics information for the active menu.

Table 64
Global commands (cont'd.)

Command	Action
lines <n>	Set the number of lines (n) that display on the screen at one time. **TIP:** The default value is 24 lines. When used without a value, the current setting.
verbose <n>	Sets the level of information displayed on the screen: 0 = Quiet: Nothing appears except errors—not even prompts. 1 = Normal: Prompts and requested output are shown without menus. 2 = Verbose: Everything is shown. **TIP:** The default level is 2. When used without a value, the current setting .

Command line history and editing

You can use the CLI to retrieve and modify commands entered previously. Table 65 "Command line history and editing options" (page 416) lists options that are available globally at the command line.

Table 65
Command line history and editing options

Option	Description
history	Display a numbered list of the 10 most recent commands.
!!	Repeat the most recent command.
! <n>	Repeat the *n* th command shown on the history list.
popd	Return to a position in the menu structure that was bookmarked using the **pushd** command.
Ctrl+p	Recall previous command from the history list. **TIP:** You can also use the up arrow key. You can use this command to regress through the last 10 commands. The recalled command can be executed as is, or edited using the options in this table.
Ctrl+n	Recall next command from the history list. **TIP:** You can also use the down arrow key. Use this command to proceed through the next 10 commands. The recalled command can be executed as is, or edited using the options in this table.
Ctrl+a	Move cursor to the beginning of the command line.
Ctrl+e	Move cursor to the end of the command line.

Table 65
Command line history and editing options (cont'd.)

Option	Description
Ctrl+b	Move the cursor back, one position to the left. You can also use the left arrow key.
Ctrl+f	Move the cursor forward, one position to the right. You can also use the right arrow key.
Backspace	Erase one character to the left of the cursor position. You can also use the **Delete** key.
Ctrl+d	Delete one character at the cursor position.
Ctrl+k	Kill (erase) all characters from the cursor position to the end of the command line.
Ctrl+l	Rewrite the most recent command.
Ctrl+c	Abort an on-going transaction. **TIP:** Press **Ctrl+c** when there is no on-going transaction, in order to display the current menu. **ATTENTION** Pressing **Ctrl+c** does not abort screen output generated by the **cur** command. Press **q** to abort the extensive screen output that may result from the **cur** command.
Ctrl+u	Clear the entire line.
Other keys	Insert new characters at the cursor position.

CLI shortcuts

You can use the following CLI command shortcuts:

- "Command stacking" (page 417)
- "Command abbreviation" (page 418)
- "Tab completion" (page 418)
- "Using a submenu name as a command argument" (page 418)

Command stacking

To access a submenu and one of the related menu options, you can type multiple commands, separated by forward slashes (/), on a single line.

For example, to access the **list** command in the NTP Servers menu from the Main menu prompt, use the following keyboard shortcut:

```
>> Main# cfg/sys/time/ntp/list
```

You can also use command stacking to proceed one or more levels in the menu system, and go directly to another submenu and one of the related menu options in that submenu.

For example, to proceed two levels (from the NTP Servers menu to the System menu) and then go to the DNS settings menu to access the DNS servers menu, use the following command:

```
>> NTP Servers# ../../dns/servers
```

Command abbreviation

You can abbreviate most commands.

To abbreviate a command, type the first characters which distinguish the command from the others in the same menu or submenu.

For example, you can abbreviate the following command:

```
>> Main# cfg/sys/time/ntp/list
```

to

```
>> Main# c/sy/t/n/l
```

Tab completion

The Tab key can be used in the following ways:

- To search for CLI commands or options:
  - At the menu prompt, type the first character of a command. **TIP:** You can use additional characters to refine the search.
  - Press Tab.
    A list of commands that begin with the character you selected . If only one command matches the character you typed, that command on the command line when you press Tab. Press ENTER to execute the command.
- To display the active menu:
  - Ensure that the command line is blank.
  - At the menu prompt, press the Tab key.

Using a submenu name as a command argument

To display the properties related to a specific submenu, you can include the submenu name as an argument to the **cur** command (at a menu prompt one level up from the desired submenu information).

For example, to display system information at the Configuration menu prompt, without descending into the System menu (**/cfg/sys**), use the following command:

```
>> Configuration# cur sys
```

```
>> Configuration# cur sys
System:
  Management IP (MIP) address = 192.168.128.211

iSD Host 1:
Type of the iSD = master
IP address = 192.168.128.213
License =
IPSEC user sessions:  250
Secure Service Partitioning
PortalGuard
TPS: unlimited
SSL user sessions:  250
Default gateway address = 192.168.128.3
Ports = 1 :  2
Hardware platform = 3070
Host Routes:
No items configured
Host Interface 1:
IP address = 192.168.128.213
Network mask = 255.255.255.0
VLAN tag id = 0
Mode = failover
Primary port = 0
Interface Ports:
1
Host Port 1:
Autonegotiation = on
```

If you use the **cur** command without the **sys** submenu argument, information related to the Configuration menu and all submenus .

Using slashes and spaces in commands

To include a forward slash (/) or a space in a command string, place the string containing the slash or space within double quotation marks before you execute the command.

For example, to specify a directory path and file name on the same line as the **ftp** command in the CLI, double quotation marks are required:

```
>> Software Management# download ftp 10.0.0.1
"pub/SSL-5.1.1-upgrade_complete.pkg"
```

IP address and network mask formats

IP addresses and network masks can be expressed in different ways in the CLI.

IP addresses

IP addresses can be specified in the following ways:

- Dotted decimal notation—specify the IP address as is: **10.0.0.1**
- According to the formats below:
  - **A.B.C.D** = A.B.C.D, the equivalent of dotted decimal notation
  - **A.B.D** = A.B.0.D — that is, **10.1.10** translates to 10.1.0.10
  - **A.D** = A.0.0.D — that is, **10.1** translates to 10.0.0.1
  - **D** = 0.0.0.D — that is, **10** translates to 0.0.0.10

Network masks

A network mask can be specified in dotted decimal notation or as number of bits. Where the network mask is:

- **255.0.0.0** it can also be expressed as **8**
- **255.255.0.0** it can also be expressed as **16**
- **255.255.255.0** it can also be expressed as **24**
- **255.255.255.255** it can also be expressed as **32**

Variables

You can use variables in some commands and features in the Nortel SNAS software.

TIP: Variables included in links are URL encoded. Variables included in static texts are not URL encoded.

Table 66 "Variables" (page 420) describes variables and their use.

Table 66
Variables

Variable	Use
<var:user>	Expands to the user name specified when the user logged on to the domain.
<var:password>	Expands to the password specified when the user logged on to the domain.
<var:group>	Expands to the group to which the logged on user is a member.

Table 66
Variables (cont'd.)

Variable	Use
<var:portal>	Expands to the Portal IP address. **TIP:** The variable can be included in redirect URLs.
<var:domain>	Expands to the domain name specified for the authentication method of the logged on user.
<var:method>	Expands to the access protocol used (http or https).
<var:sslsid>	Expands to the SSL session ID in binary format.
<md5:...>	Expands the variable or variables (for example, <md5:<user>:<password>>) and computes an MD5 checksum which is Base 64 encoded. **TIP:** Can be used when creating dynamic HTTP headers.
<base64:...>	Expands the variable or variables (for example, <base64:<user>:<password>>) and encodes them using Base 64. **TIP:** Can be used when creating dynamic HTTP headers.
<var:nhaFailureReason>	Expands to the Nortel Health Agent rule expression and the Nortel Health Agent rule comment specified for the current SRS rule when a Nortel Health Agent check has failed.
<var:nhaFailureDetail>	Expands to the software definition comment specified for the current SRS rule, including additional failure details, when a Nortel Health Agent check has failed.
Operator-defined variables	Custom variables can be created to retrieve the desired values from RADIUS and LDAP databases.

CLI Main Menu

The Main menu appears after a successful connection and login. Figure 32 "CLI main menu" (page 421) represents the Main menu as it appears when logged on as Administrator. Note that some of the commands are not available when logged on as Operator.

Figure 32
CLI main menu

```
[Main Menu]
      info         - Information menu
      stats        - Statistics menu
      cfg          - Configuration menu
      boot         - Boot menu
      maint        - Maintenance menu
      diff       - Show pending config changes   [global command]
      apply      - Apply pending config changes  [global command]
      revert     - Revert pending config changes [global command]
      paste      - Restore saved config with key [global command]
      help        - Show command help            [global command]
      exit         - Exit [global command, always available]
```

CLI command reference

The following CLI menus are accessible from the Main menu:

- Information—provides submenus for displaying information about the current status of the Nortel Secure Network Access Switch. For the Information menu commands, see “Information menu” (page 422).
- Statistics—provides submenus for displaying Nortel SNAS performance statistics. For the Statistics menu commands, see “Statistics menu” (page 423).
- Configuration—provides submenus for configuring the Nortel SNAS cluster. Some of the commands in the Configuration menu are available only when logged on as Administrator. For the Configuration menu commands, see “Configuration menu” (page 424).
- Boot—used for upgrading Nortel SNAS software and for rebooting Nortel SNAS devices. The Boot menu is accessible only when logged on as Administrator. For the Boot menu commands, see “Boot menu” (page 448).
- Maintenance—used for sending technical support information to an external file server. For the Maintenance menu commands, see “Maintenance menu” (page 449).

Information menu

The Information menu contains commands used to display current information about the Nortel SNAS system status and configuration. Table 67 "Information menu commands" (page 422) lists the Information commands in alphabetical order.

Table 67
Information menu commands

Command	Parameters/Submenus	Purpose

`/info`	`certs`
	`sys`
	`sonmp`
	`licenses`
	`kick <user> <addr> <group>`
	`blacklist`
	`domain [<domain ID>]`
	`switches`
		View current information about system status and the system configuration.

Command	Parameters/Submenus	Purpose
	dist [<hostid>] ip <ipaddr>|<option> mac <macaddr>|<option> sessions [<domainid> <switchid> [<username-prefix>]] groupsessi <groupname> dhcp [<list> [<addr> <subnet> <all>]] [<del> [<addr> <subnet> <all>]] <stats> snmp-profi switch [<domainid>] [<switchid>] contlist [<Exclude buffers+cache from mem util: [yes/no]>] local ethernet ports	
/info/events	alarms download <protocol> <server> <filename>	View active alarms.
/info/logs	list download <protocol> <server> <filename>	View and download log files.

Statistics menu

The Statistics menu contains commands used to view statistics for the Nortel SNAS cluster and individual hosts. Table 68 "Statistics menu commands" (page 424) lists the Statistics commands in alphabetical order.

Table 68
Statistics menu commands

Command	Parameters/Submenus	Purpose
`/stats`		View performance statistics for the cluster and for individual Nortel SNAS hosts.
`/stats/aaa`	`total` `isdhost <host ID> <domain ID> dump`	View authentication statistics for the Nortel SNAS cluster or for individual Nortel SNAS hosts.
`/stats/dump`		View all available statistics for the Nortel SNAS cluster.

Configuration menu

The Configuration menu contains commands used to configure the Nortel SNAS. Table 69 "Configuration menu commands" (page 424) lists the configuration commands in alphabetical order.

Table 69
Configuration menu commands

Command	Parameters/Submenus	Purpose

`/cfg/cert <cert ID>`	`name <string>`
	`cert`
	`key`
	`revoke`
	`gensigned`
	`request`
	`sign`
	`test`
	`import <protocol> <server> <certfile>`
	`export`
	`display [<encrypt private key yes|no> <export pass phrase> <reconfirm export pass phrase>]`
		Manage private keys and certificates and access the Certificate menu.

Command	Parameters/Submenus	Purpose
	show **info** **subject** **validate** **keysize** **keyinfo** **del**	
/cfg/cert <cert ID>/revoke	**add <integer>** **addx <integer>** **del <integer>** **list** **rev** **import <protocol> <server> <file>** **automatic**	Access the Revocation menu.
/cfg/cert <cert ID>/revoke/automatic	**url <url>** **authDN <LDAP-Distinguished-Name>** **passwd <password>** **interval <time>** **cacerts** **ena [<enabled|disabled>]** **dis [<enabled|disabled>]**	Access the Automatic CRL menu.
/cfg/domain <domain ID>	**name <name>** **pvips <IPaddr>** **aaa** **location** **patchlink** **server** **portal** **linkset**	Configure the domain.

Command	Parameters/Submenus	Purpose
	switch snmp-profi vlan dhcp sshkey dnscapt httpredir radius nap quick syslog adv del	
/cfg/domain #/aaa/auth <auth ID>	type radius|ldap|ntlm|sitemi nder|cleartrust|cert|r sa|local name <name> display radius|ldap|ntlm|sitemi nder|cleartrust|cert|r sa|local adv del	Create and configure an authentication method.
/cfg/domain #/aaa/auth <auth ID>/adv	groupauth <auth IDs>	Configure the current authent ication scheme to retrieve user group information from a different authentication scheme.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/auth <auth ID> (for LDAP)		Configure the Nortel SNAS domain to use an external LDAP server for authentication.
/cfg/domain #/aaa/auth <auth ID>/ldap	**servers** **searchbase <DN>** **groupattr <names>** **userattr <names>** **isdbinddn <DN>** **isdbindpas <password>** **ldapmacro** **enaldaps true|false** **ldapscert** **enauserpre true|false** **enacutdoma** **enashortgrp <enable short group format > <auth ID>** **groupsearc** **timeout <interval>** **activedire** **adv**	Modify settings for the specific LDAP configuration.
/cfg/domain #/aaa/auth <auth ID>/ldap/activedire	**enaexpired true|false** **expiredgro <group>** **exppasgrou <group name>** **recursivem true|false**	Manage clients whose passwords have expired or who need to change their passwords,

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/auth <auth ID>/ldap/ldapmacro	list <name> <attrname> <prefix> <suffix> del <index number> add <name> <attrname> <prefix> <suffix> insert <position> <name> <attrname> <prefix> <suffix> move <index number> <new index number>	Configure LDAP macros.
/cfg/domain #/aaa/auth <auth ID>/ldap/servers	list <ip> <port> del <index number> add <ip> <port> insert <position> <ip> <port> move <index number> <new index number>	Manage the LDAP servers used for client authentication in the domain.
/cfg/domain #/aaa/auth <auth ID>/ldap/groupsearc	groupbase <distinguished-name> memberattr <string> ena [<enabled|disabled>] dis [<enabled|disabled>]	
/cfg/domain #/aaa/auth <auth ID>/ldap/adv	enaxfilter <true|false> xfilteratt <string> xfilterval <string>	
/cfg/domain #/aaa/auth <auth ID> (for local portal database)		Create the Local authentication method.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/auth <auth ID>/local	**add <user name> <password> <group>** **passwd <user name> <password>** **groups <user name> <desired group>** **radattr <add> <list> <del>** **del <user name>** **list <prefix>** **import <protocol> <host> <filename>** **export <protocol> <host> <filename>**	Manage client users and their passwords in the local portal database.
/cfg/domain #/aaa/auth <auth ID> (for local MAC database)	**add <MAC address> <user name> <IP type> <dhcp> <static> [<device type> [<PC> <phone> <passive>]] <IP address> <switch IP address> <switch unit> <switch port> <group names> <comments>** **del <MAC address>** **list** **show <mac>** **import <protocol> <host> <filename>** **export <protocol> <host> <filename>** **clear**	Manage the local MAC database
/cfg/domain #/aaa/auth <auth ID> (for RADIUS)		Configure the domain to use an external RADIUS server for authentication.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/auth <auth ID>/radius	servers vendorid <vendor ID> vendortype <vendor type> domainid <domain ID> domaintype <domain type> authproto pap | chapv2 timeout <interval> sessiontim	Modify settings for the specific RADIUS configuration.
/cfg/domain #/aaa/auth <auth ID>/radius/servers	list <ip> <auth_port> <acct_port> <secret> del <index number> add <ip> <auth_port> <acct_port> <secret> insert <position> <ip> <auth_port> <acct_port> <secret> move <index number> <new index number>	Manage the RADIUS servers used for client authentication in the domain.
/cfg/domain #/aaa/auth <auth ID>/radius/sessiontim	vendorid <vendor ID> vendortype <vendor type> ena [<bool>] dis [<bool>]	Configure the Nortel SNAS for session timeout.
/cfg/domain #/aaa/authorder <auth ID>[,<auth ID>]		Specify the authentication fallback order.
/cfg/domain #/aaa/defgroup <group name>		Create a default group to which users are assigned if they are not associated with a specific group in the authentication database.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/filter <filter ID>	name <name> nha true|false|ignore nap true|false|ignore patchlink true|false|ignore comment <comment> del	Configure the client filters, which determine whether extended profile data will be applied to a user.
/cfg/domain #/aaa/group <group ID>	name <name> locations radattr restrict sessionttl linkset extend <profile ID> srs <SRS rule name> mactrust <blacklist | bypass | none> agentmode <runonce | continuous | never> macreg <true | false> reguser enftype <filter_only | vlan_filter> cachepass admrights <user> <passwd> <action> <reset> syscredent comment <comment> del	Configure groups on the domain.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/group #/extend [<profile ID>]	filter <name> vlan <ID|name> acl <string> radattr linkset del	Configure the extended profiles for a group.
/cfg/domain #/aaa/group #/extend #/linkset	list <name> del <index number> add <linkset name> insert <position> <linkset name> move <index number> <new index number>	Map predefined linksets to an extended profile.
/cfg/domain #/aaa/group #/linkset	list <name> del <index number> add <name> insert <position> <name> move <index number> <new index number>	Map predefined Linksets to a group.
/cfg/domain #/aaa/group #/radattr	list <vendor> <id> <value> del <index number> add <vendor> <id> <value> insert <position> <vendor> <id> <value> move <index number> <new index number>	Map predefined RADIUS attributes to a group.

Command	Parameters/Submenus	Purpose
cfg/domain #/aaa/group #/syscredent	user <sys_user> passwd prevuser <sys_user> prevpasswd actdate <YYYY MM DD HH:MM|NN [s|m|h|d]> earlpush <YYYY MM DD HH:MM|NN [s|m|h|d]> exprprev updclients <bool> reset <confirm> ena [<true|false>] dis [<true|false>]	
cfg/domain #/aaa/group #/cachepass	Usage: cachepass <true|false>	
/cfg/domain #/aaa/radacct	servers domainattr ena dis	Configure the Nortel SNAS to support RADIUS accounting.
/cfg/domain #/aaa/radacct/servers	list <ip> <port> <secret> del <index number> add <ip> <port> <secret> insert <position> <ip> <port> <secret> move <index number value> <new index number value>	Configure the Nortel SNAS to use external RADIUS accounting servers.

Command	Parameters/Submenus	Purpose
/cfg/domain #/aaa/radacct/domainattr	vendorid vendortype	Configure vendor-specific attributes in order to identify the Nortel SNAS domain.
/cfg/domain #/aaa/nha	quick recheck <interval> heartbeat <interval> hbretrycnt <count> status-quo on|off onflysrs on|off desktopage desktopagent <on|off|auto> desktopnam Desktop agent shortcut name action teardown|restricted list details on|off custscript on|off persistoob on|off loglevel fatal|error|warning|info|debug	Configure settings for the Nortel Health Agent host integrity check and the check result.
/cfg/domain #/aaa/nha/quick		Configure settings for the SRS rule check using the Nortel Health Agent quick setup wizard.
/cfg/domain #/adv	interface <integer> log <all | login | http | portal | reject>	Map a backend interface to the domain and configure logging options,

Command	Parameters/Submenus	Purpose
/cfg/domain #/del		Remove the current domain from the system configuration.
/cfg/domain #/dhcp	subnet stdopts Enter the standard options menu vendopts Enter the standard options menu (<number> <name> <value> <del> quick	Configure local DHCP services
/cfg/domain #/dhcp	subnet <number> [<type> [<hub> [<type> <name> <address> <netmask> <phone> <relaygreen> <vlan> <red ranges|std opts|vendopts> <yellow ranges|stdopts|vendo pts> <green ranges|st dopts|vendopts> <ena> <dis> <del>]] [<filter> [<type> <name> <address> <netmask> <known> <unknown> <ena> <dis> <del>]] [<standard> [<type> <name> <address> <netmask> <settings> <ena> <dis> <del>]]]> <name> <address> <netmask> stdopts Enter the standard options menu vendopts Enter the standard options menu (<number> <name> <value> <del> quick	Configure local DHCP services

Command	Parameters/Submenus	Purpose
/cfg/domain #/dhcp/subnet	type name address netmask phone <phone signature> relaygreen <set external DHCp server> vlan <vlan mane> <red ranges|stdopts|vendopts> <yellow ranges|stdopts|vendopts> <green ranges|stdopts|vendopts> ena [<enabled|disabled>] dis [<enabled|disabled>] del	Configure local DHCP subnet services
/cfg/domain #/dnscapt	exclude ena dis	Configure the Nortel SNAS portal as a captive portal.
/cfg/domain #/dnscapt/exclude	list del <index name> add <domain name> insert <index number> <domain name> move <index number> <new index number>	Create and manage the Exclude List.
/cfg/domain #/httpredir	port <integer> redir on|off	Configure the domain to automatically redirect HTTP requests to the HTTPS server specified for the domain.

Command	Parameters/Submenus	Purpose
/cfg/domain #/linkset <linkset ID>	name <name> text <text> autorun true|false link <index> del	Create and configure a linkset.
/cfg/domain #/linkset #/link <index>	move <new index> text <text> type external external del	Create and configure the links included in the linkset.
/cfg/domain #/linkset #/link #/external/quick		Launch the wizard to configure settings for a link to an external web page.
/cfg/domain #/portal	import <protocol> <server> <filename> restore banner redirect <URL> logintext <text> iconmode clean|fancy linktext <text> linkurl on|off linkcols <columns> linkwidth <width> companynam <string> colors content lang ieclear on|off	Modify the look and feel of the portal page that in the client's web browser.

Command	Parameters/Submenus	Purpose
/cfg/domain #/portal/colors	color1 <code> color2 <code> color3 <code> color4 <code> theme default|aqua|apple| jeans|cinnamon|candy	Customize the colors used for the portal display.
/cfg/domain #/portal/content	import <protocol> <host> <file> export <protocol> <host> <filename> delete <yes|no> available show ena [<bool>] dis [<bool>]	Add custom content, such as Java applets, to the portal.
/cfg/domain #/portal/lang	setlang <lang> charset list [<prefix>] beconv	Set the preferred language for the portal display.
/cfg/domain #/portal/lang/beconv	add <protocol smb|ftp> <host> del <number> list	Configures the backend conversion.
/cfg/domain #/quick		Launch the quick switch setup wizard to add network access devices to the domain.
/cfg/domain #/server	port <port> interface <interface ID> dnsname <name> trace ssl adv	Configure the portal server used in the domain.

Command	Parameters/Submenus	Purpose
/cfg/domain #/server/adv/traflog	sysloghost <IPaddr> udpport <port> protocol ssl2|ssl3|ssl23|tls1 priority debug|info|notice ena dis	Set up a syslog server to receive UDP syslog messages for all HTTP requests handled by the portal server.
/cfg/domain #/server/ssl	cert <certificate index> cachesize <sessions> cachettl <ttl> cacerts <certificate index> cachain <certificate index list> protocol ssl2|ssl3|ssl23|tls1 verify none|optional|required ciphers <cipher list> ena dis	Configure SSL-specific settings for the portal server.
/cfg/domain #/server/trace	ssldump tcpdump ping <host> dnslookup <host> traceroute <host>	Verify connectivity and capture information about SSL and TCP traffic between clients and the portal server.
/cfg/domain #/sshkey	generate show export <protocol> <host> <filename>	Generate, view, and export the public SSH key for the domain.

Command	Parameters/Submenus	Purpose
/cfg/domain #/switch <switch ID>	name <name> ip <IPaddr> mgmtproto <sscp|sscplite> type ERS8300|ERS5500|ERS4500 port <port> hlthchk vlan rvid <VLAN ID> sshkey ena dis delete	Configure the network access devices on the domain.
/cfg/domain #/switch #/dis		Stop communication between the Nortel SNAS and a network access devices.
/cfg/domain #/switch #/ena		Restart communication between the Nortel SNAS and a network access devices.
/cfg/domain #/switch #/hlthchk	interval <seconds> deadcnt <count> sq-int <seconds>	Configure the interval and dead count parameters for the Nortel SNAS health checks and status-quo mode.
/cfg/domain #/switch #/sshkey	import add del show export user <user>	Retrieve the public key for the network access devices and export the public key for the domain.

Command	Parameters/Submenus	Purpose
/cfg/domain #/switch #/vlan	add <name> <VLAN ID> del <index> list	Manage the VLAN mappings for a specific network access devices.
/cfg/domain #/vlan	add <name> <VLAN ID> del <index> list	Manage the VLAN mappings for all the network access devices in the domain.
/cfg/dump		Perform a configuration dump.
/cfg/gtcfg	<protocol> <host> <filename>	Restore the system configuration.
/cfg/lang	import <protocol> <server> <filename> <code> export <protocol> <server> <filename> list vlist [<letter>] del <code>	Manage the language definition files in the system.
/cfg/ptcfg	<protocol> <host> <filename>	Save the system configuration to a file on a file exchange server.
/cfg/quick		Create a domain using the Nortel SNAS quick setup wizard.
/cfg/sys	mip <IPaddr> host <host ID> routes time dns rsa <server ID> syslog accesslist adm user	View and configure cluster-wide system settings.

Command	Parameters/Submenus	Purpose
	distrace	
/cfg/sys/accesslist	list del <index number> add <IPaddr> <mask>	Manage the Access List in order to control Telnet and SSH access to the Nortel SNAS cluster.
/cfg/sys/adm	snmp sonmp on|off clitimeout <interval> audit auth abl hardenpass telnet on|off ssh on|off srsadmin http https sshkeys redist <yes|no>	Configure administrative settings for the system.
/cfg/sys/adm/audit	servers vendorid <vendorid> vendortype <vendortype> ena dis	Configure the Nortel SNAS to support RADIUS auditing.
/cfg/sys/adm/audit/servers	list <ip> <port> <secret> del <index> add <ip> <port> <secret> insert <position> <ip> <port> <secret> move <index number value> <new index number value>	Configure the Nortel SNAS to use external RADIUS audit servers.

Command	Parameters/Submenus	Purpose
/cfg/sys/adm/auth	servers timeout <interval> fallback on|off ena [<true|false>] dis [<true|false>]	Configure the Nortel SNAS to support RADIUS authentication of system users.
/cfg/sys/adm/auth/servers	list <ip> <port> <secret> del <index> add <ip> <port> <secret> insert <position> <ip> <port> <secret> move <index number value> <new index number value>	Configure the Nortel SNAS to use external RADIUS servers to authenticate system users.
/cfg/sys/adm/abl	users <list> <add> <delete> host <list> <add> <delete> user_atmpt <attempts/timeperiod> host_atmpt <attempts/timeperiod> user_perge time period <<integer>[hd]> host_perge time period <<integer>[hd]> show clear ena [<true|false>] dis [<true|false>]	Configure the Nortel SNAS to support auto blacklisting.

Command	Parameters/Submenus	Purpose
/cfg/sys/adm/hardenpass	length <integer> lowercase <integer> uppercase <integer> digits <integer> others <integer> retry <integer> ena [<true|false>] dis [<true|false>]	Configure the Nortel SNAS to support harden password.
/cfg/sys/adm/http	port <integer> ena [<true|false>] dis [<true|false>]	Configure the Nortel SNAS to support http settings.
/cfg/sys/adm/https	port <integer> ena [<true|false>] dis [<true|false>]	Configure the Nortel SNAS to support https settings.
/cfg/sys/adm/snmp		Configure SNMP for the Nortel SNAS network.
/cfg/sys/adm/snmp	ena [<true|false>] dis [<true|false>] versions <v1|v2c|v3> snmpv2-mib community users <id> target <nr> event	Configure SNMP management of the Nortel SNAS cluster.
/cfg/sys/adm/snmp/community	read <name> write <name> trap <name>	Configure the community aspects of SNMP monitoring.

Command	Parameters/Submenus	Purpose
/cfg/sys/adm/snmp/event	addmonitor [-c Comment] [-f Freq] [-o OID]* [-b |-t | -x ...] Name Oid ... delmonitor <name> addevent [-c Comment>] Name Notification [OID...] delevent <name> list	Configure monitors and events defined in the DISMAN-EVENT-MIB.
/cfg/sys/adm/snmp/snmpv2-mib	sysContact <contact> snmpEnable disabled|enabled	Configure parameters in the standard SNMPv2 MIB.
/cfg/sys/adm/snmp/target <target ID>	ip <IPaddr> port <port> version v1|v2c|v3 del	Configure notification targets.
/cfg/sys/adm/snmp/users <user ID>	name <name> seclevel none|auth|priv permission get|set|trap authproto md5|sha authpasswd <password> privproto des|aes privpasswd <password> del	Manage SNMPv3 users in the Nortel SNAS configuration.
/cfg/sys/adm/srsadmin	port <port> ena dis	Configure support for managing the SRS rules.
/cfg/sys/adm/sshkeys	generate show knownhosts	Generate and view the SSH keys used by all hosts in the cluster for secure management communications.

Command	Parameters/Submenus	Purpose
/cfg/sys/adm/sshkeys/knownhosts	list del <index number> add import <IPaddr>	Manage the public SSH keys of known remote hosts.
/cfg/sys/dns	servers cachesize <entries> retransmit <interval> count <count> ttl <ttl> health <interval> hdown <count> hup <count>	Configure DNS settings for the cluster.
/cfg/sys/dns/servers	list del <index number> add <IPaddr> insert <index number> <IPaddr> move <index number> <new index number>	Configure the cluster to use external DNS servers.
/cfg/sys/host #/interface #/ports	list del <port> add <port>	View and manage the ports assigned to an interface.
/cfg/sys/host #/interface #/routes	list del <index number> add <IPaddr> <mask> <gateway>	Manage static routes for a particular interface.
/cfg/sys/host #/interface <interface ID>	ip <IPaddr> netmask <mask> gateway <IPaddr> routes vlanid <tag> mode failover|trunking ports primary <port>	Configure an IP interface and assign physical ports on a particular Nortel SNAS host,

Command	Parameters/Submenus	Purpose
	delete	
/cfg/sys/host #/port <port>	**autoneg on|off** **speed <speed>** **mode full|half**	Configure the connection properties for a port.
/cfg/sys/host #/routes		Manage static routes for a particular Nortel SNAS host when more than one interface is configured.
/cfg/sys/host <host ID>	**ip <IPaddr>** **sysName <name>** **sysLocation <location>** **license** **gateway <IPaddr>** **routes** **interface <interface number>** **port <nr>** **ports** **hwplatform** **halt <confirm>** **reboot <confirm>** **delete**	Configure basic TCP/IP properties for a particular Nortel SNAS device in the cluster,
/cfg/sys/routes		Manage static routes on a cluster-wide level when more than one interface is configured.
/cfg/sys/rsa	**rsaname <name>** **import <protocol> <host> <filename>** **rmnodesecr** **del**	Configure the symbolic name for the RSA server and import the sdconf.rec configuration file.

Command	Parameters/Submenus	Purpose
/cfg/sys/syslog	list <ip> <n> del <index> add <ip> <n> insert <position> <ip> <n> move <index number value> <new index number value>	Configure syslog servers for the cluster.
/cfg/sys/time	date <date> time <time> tzone <timezone> ntp	Configure date and time settings for the cluster.
/cfg/sys/time/ntp	list <ip> del <index> add <ip>	Manage NTP servers used by the system.
/cfg/sys/user	passwd expire <DDdHHhMMmSS> list del <username> add <username> edit <username> caphrase	Change the password for the currently logged on user and add or delete user accounts.
/cfg/sys/user/edit <username>	groups cur	Set or change the login password for a specified user and view and manage group assignments.
/cfg/sys/user/edit <username>/groups	list del <group index> add admin|oper|certadmin	Set or change a user's group assignment.

Boot menu

The Boot menu contains commands for management of Nortel SNAS software and devices. Table 70 "Boot menu commands" (page 449) lists the boot commands in alphabetical order.

Table 70
Boot menu commands

Command	Parameters/Submenus	Purpose
/boot	software halt <confirm> reboot <confirm> delete	Manage Nortel SNAS software and devices.
/boot/software	cur <version> <name> <status> activate <software version> download <protocol> <host> <fname> del <confirm>	View, download, and activate software versions for the Nortel SNAS device to which you are connected.

Maintenance menu

The Maintenance menu contains commands used to perform maintenance and management activities for the system and individual Nortel SNAS devices. Table 71 "Maintenance menu commands" (page 449) lists the Maintenance commands.

Table 71
Maintenance menu commands

Command	Parameters/Submenus	Purpose
/maint	log dumplogs <protocol> <host> <filename> <all-isds?> dumpstats <protocol> <host> <filename> <all-isds?> chkcfg list | chkcfg [all-isds |one-isds] [item...] [syslog] starttrace <tags (all|aaa|dhcp|dns|ssl|tg|snas|patchlink|radius|nap)> [<domain ID>] stoptrace	Check the applied configuration and download log file and system status information for technical support purposes.
/maint/log	in-memory <start-log> <stop-log> <displaylog> <clearlog>	

Appendix Syslog messages

This appendix contains a list of the syslog messages that are sent from the Nortel SNAS to a syslog server, when a syslog server has been added to the system configuration. For more information about adding a syslog server to the system configuration, see “Configuring syslog servers” (page 279).

The syslog messages are presented in two ways:

- “Syslog messages by message type” (page 451)
- “Syslog messages in alphabetical order” (page 465)

Syslog messages by message type

The following types of messages occur:

- operating system (OS) (see “Operating system (OS) messages” (page 452))
- system control (see “System Control Process messages” (page 453))
- traffic processing (see “Traffic Processing Subsystem messages” (page 457))
- start-up (see “Start-up messages” (page 461))
- AAA (see “AAA subsystem messages” (page 461))
- NSNAS (see “NSNAS subsystem messages” (page 463))

Operating system (OS) messages

There are three categories of operating system (OS) system messages:

- EMERG (see Table 72 "Operating system messages—EMERG" (page 452))
- CRITICAL (see Table 73 "Operating system messages—CRITICAL" (page 452))
- ERROR (see Table 74 "Operating system messages—ERROR" (page 453))

Table 72 "Operating system messages—EMERG" (page 452) lists the EMERG operating system messages.

Table 72
Operating system messages—EMERG

Message	Category	Explanation/Action
Root filesystem corrupt	EMERG	The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover.
Config filesystem corrupt beyond repair	EMERG	The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover.
Failed to write to config filesystem	EMERG	Probable hardware error. Reinstall.

Table 73 "Operating system messages—CRITICAL" (page 452) lists the operating system CRITICAL messages.

Table 73
Operating system messages—CRITICAL

Message	Category	Explanation/Action
Config filesystem re-initialized - reinstall required	CRITICAL	Reinstall.
Application filesystem corrupt - reinstall required	CRITICAL	Reinstall.

Table 74 "Operating system messages—ERROR" (page 453) lists the operating system EMERG messages.

Table 74
Operating system messages—ERROR

Message	Category	Explanation/Action
Config filesystem corrupt	ERROR	Possible loss of configuration. Followed by the message: `Config filesystem re-initialized - reinstall required` or `Config filesystem restored from backup`.
Missing files in config filesystem	ERROR	Possible loss of configuration. Followed by the message: `Config filesystem re-initialized - reinstall required` or `Config filesystem restored from backup`.
Logs filesystem re-initialized	ERROR	Loss of logs.
Root filesystem repaired - rebooting	ERROR	fsck found and fixed errors. Probably OK.
Config filesystem restored from backup	ERROR	Loss of recent configuration changes.
Rebooting to revert to permanent OS version	ERROR	Happens after `Config filesystem re-initialized - reinstall required` or `Config filesystem restored from backup` if software upgrade is in progress (in other words, if failure at first boot on new OS version).

System Control Process messages

There are three categories of System Control Process messages:

- INFO (see Table 75 "System control process messages—INFO" (page 454))
- ALARM (see Table 77 "System Control Process messages—ALARM" (page 455))
- EVENT (see Table 78 "System Control Process messages—EVENT" (page 456))

Events and alarms are stored in the event log file. You can access the event log file by using the **`/info/events/download`** command. You can view active alarms by using the **`/info/events/alarms`** command. For more information, see “Viewing system information and performance statistics” (page 337).

Table 75 "System control process messages—INFO" (page 454) lists the System Control Process INFO messages.

Table 75
System control process messages—INFO

Message	Category	Explanation/Action
System started [isdssl-<version>]	INFO	Sent whenever the system control process has been (re)started.

About alarm messages

Alarms are sent at a syslog level corresponding to the alarm severity shown in Table 76 "Alarm severity and syslog level correspondence" (page 454).

Table 76
Alarm severity and syslog level correspondence

Alarm severity	Syslog level
CRITICAL	ALERT
MAJOR	CRITICAL
MINOR	ERROR
WARNING	WARNING
*	ERROR

Alarms are formatted according to the following pattern:

Id: <alarm sequence number>
Severity: <severity>
Name: <name of alarm>
Time. <date and time of the alarm>
Sender: <sender, e.g. system or the Nortel SNAS device's IP address>
Cause: <cause of the alarm>
Extra: <additional information about the alarm>

When an alarm is cleared, one of the following messages is sent:

- Alarm Cleared Name="<Name>" Id= "<ID>" Sender="<Sender>"
- Alarm Cleared Id="<ID>"

Table 77 "System Control Process messages—ALARM" (page 455) lists the System Control Process ALARM messages. To simplify finding the alarm messages, the name parameter is listed first.

Table 77
System Control Process messages—ALARM

Message	Category	Explanation/Action
Name: isd_down Sender: <IP> Cause: down Extra: Severity: critical	ALARM	A member of the Nortel SNAS cluster is down. This alarm is only sent if the cluster contains more than one Nortel SNAS.
Name: single_master Sender: system Cause: down Extra: Severity: warning	ALARM	Only one master Nortel SNAS in the cluster is up and running.
Name: log_open_failed Sender: <IP>, event Cause and Extra are explanations of the fault. Severity: major	ALARM	The event log (where all events and alarms are stored) could not be opened.
Name: make_software_release_permanent_failed Sender: <IP> Cause: file_error | not_installed Extra: "Detailed info" Severity: critical	ALARM	Failed to make a new software release permanent after being activated. The system automatically reverts to the previous version.
Name: copy_software_release_failed Sender: <IP> Cause: copy_failed | bad_release_package | no_release_package | unpack_failed Extra: "Detailed info" Severity: critical	ALARM	A Nortel SNAS failed to install a software release while trying to install the same version as all other Nortel SNAS devices in the cluster. The failing Nortel SNAS tries to catch up with the other cluster members, because it was not up and running when the new software version was installed.
Name: license Sender: license_server Cause: license_not_loaded Extra: "All iSDs do not have the same license loaded" Severity: warning	ALARM	All Nortel SNAS devices in the cluster do not have a license containing the same set of licensed features. Check loaded licenses using the **`/cfg/sys/cur`** command.
Name: license Sender: <IP> Cause: license_expire_soon Extra: "Expires: <TIME>" Severity: warning	ALARM	The (demo) license loaded to the local Nortel SNAS expires within 7 days. Check loaded licenses using the /cfg/sys/cur command.

About event messages

Events are sent at the NOTICE syslog level. Event messages are formatted according to the following pattern:

Name: <Name>
Sender: <Sender>
Extra: <Extra>

Table 78 "System Control Process messages—EVENT" (page 456) lists the System Control Process EVENT messages.

Table 78
System Control Process messages—EVENT

Message	Category	Explanation/Action
Name: partitioned_network Sender and Extra is lower level information.	EVENT	Indicates that a Nortel SNAS is recovering from a partitioned network situation.
Name: ssi_mipishere Sender: ssi Extra: <IP>	EVENT	Indicates that the Management IP address (MIP) is now located at the Nortel SNAS with the <IP> host IP address.
Name: software_configuration_changed Sender: system Extra: software release version <VSN> <Status>	EVENT	Indicates that release <VSN> (version) software status is <Status> (unpacked/installed/permanent).
Name: software_release_copying Sender: <IP> Extra: copy software release <VSN> from other cluster member	EVENT	Indicates that <IP> is copying the release <VSN> from another cluster member.
Name: software_release_rebooting Sender: <IP> Extra: reboot with release version <VSN>	EVENT	Indicates that a Nortel SNAS (<IP>) is rebooting on a new release (in other words, a Nortel SNAS that was not up and running during the normal installation is now catching up).
Name: audit Sender: CLI Extra: Start <session> <details> Update <session> <details> Stop <session> <details>	EVENT	Sent when a CLI system administrator enters, exits, or updates the CLI if audit logging is enabled using the **`/cfg/sys/adm/audit/ena`** command.
Name: license_expired Sender = <IP>	EVENT	Indicates that the demo license loaded to host <IP> has expired. Check the loaded licenses with **`/cfg/sys/cur`**.

Traffic Processing Subsystem messages

There are four categories of Traffic Processing Subsystem messages:

- CRITICAL (see Table 79 "Traffic Processing messages—CRITICAL" (page 457))
- ERROR (see Table 80 "Traffic Processing messages—ERROR" (page 457))
- WARNING (see Table 81 "Traffic Processing messages—WARNING" (page 459))
- INFO (see Table 82 "Traffic Processing messages—INFO" (page 460))

Table 79 "Traffic Processing messages—CRITICAL" (page 457) lists the Traffic Processing CRITICAL messages.

Table 79
Traffic Processing messages—CRITICAL

Message	Category	Explanation/Action
DNS alarm: all dns servers are DOWN	CRITICAL	All DNS servers are down. The Nortel SNAS cannot perform any DNS lookups.

Table 80 "Traffic Processing messages—ERROR" (page 457) lists the Traffic Processing ERROR messages.

Table 80
Traffic Processing messages—ERROR

Message	Category	Explanation/Action
internal error: <no>	ERROR	An internal error occurred. Contact support with as much information as possible to reproduce this message.
javascript error: <reason> for: <host><path>	ERROR	JavaScript parsing error encountered when parsing content from <host><path>. The problem could be in the Nortel SNAS JavaScript parser, but most likely it is a syntax error in the JavaScript on the page.
vbscript error: <reason> for: <host><path>	ERROR	VBScript parsing error encountered when parsing content from <host><path>. The problem could be in the Nortel SNAS VBScript parser, but most likely it is a syntax error in the VBScript on the page.

Table 80
Traffic Processing messages—ERROR (cont'd.)

Message	Category	Explanation/Action
jscript.encode error: <reason>	ERROR	Problem encountered when parsing an encoded JavaScript. The problem could be in the Nortel SNAS JavaScript parser, or it could be a problem on the processed page.
css error: <reason>	ERROR	Problem encountered when parsing a style sheet. The problem could be in the Nortel SNAS css parser, or it could be a problem on the processed page.
Failed to syslog traffic :<reason> -- disabling traf log	ERROR	Problem occurred when the Nortel SNAS tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.
www_authenticate: bad credentials	ERROR	The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.
http error: <reason>, Request="<method> <host><path>"	ERROR	A problem was encountered when parsing the HTTP traffic. The problem indicates either a non-standard client/server or that the Nortel SNAS HTTP parser is out of sync because of an earlier non-standard transaction from the client or server on this TCP stream.
http header warning cli: <reason> (<header>)	ERROR	The client sent a bad HTTP header.
http header warning srv: <reason> (<header>)	ERROR	The server sent a bad HTTP header.
failed to parse Set-Cookie <header>	ERROR	The Nortel SNAS got a malformed Set-Cookie header from the backend web server.
Bad IP:PORT data <line> in hc script	ERROR	Bad ip:port found in health check script. Reconfigure the health script. (Normally, the CLI captures this type of problem earlier.)
Bad regexp (<expr>) in health check	ERROR	Bad regular expression found in health check script. Reconfigure the health script. (Normally, the CLI captures this type of problem earlier.)

Table 80
Traffic Processing messages—ERROR (cont'd.)

Message	Category	Explanation/Action
Bad script op found <script op>	ERROR	Bad script operation found in health check script. Reconfigure the health script. (Normally, the CLI captures this type of problem earlier.)
Connect failed: <reason>	ERROR	Connect to backend server failed with <reason>
html error: <reason>	ERROR	Error encountered when parsing HTML. Probably non-standard HTML.
socks error: <reason>	ERROR	Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.
socks request: socks version <version> rejected	ERROR	Socks request of version <version> received and rejected. Most likely a non-standard socks client.
Failed to log to CLI :<reason> -- disabling CLI log	ERROR	Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.
Can't bind to local address: <ip>:<port>: <reason>	ERROR	Problem encountered when trying to set up virtual server on <ip>:<port>.
Ignoring DNS packet was not from any of the defined names server <ip>:<port>	ERROR	Nortel SNAS received reply for non-configured DNS server.

Table 81 "Traffic Processing messages—WARNING" (page 459) lists the Traffic Processing WARNING messages.

Table 81
Traffic Processing messages—WARNING

Message	Category	Explanation/Action
DNS alarm: all dns servers are DOWN	WARNING	All DNS servers are down. The Nortel SNAS cannot perform any DNS lookups.
TPS license limit (<limit>) exceeded	WARNING	The transactions per second (TPS) limit has been exceeded.
No PortalGuard license loaded: domain <id> *will* use portal authentication	WARNING	The PortalGuard license has not been loaded on the Nortel SNAS.
No Secure Service Partitioning loaded: server <id> *will not* use interface <n>	WARNING	The Secure Service Partitioning license has not been loaded on the Nortel SNAS but the server is configured to use a specific interface.

Table 81
Traffic Processing messages—WARNING (cont'd.)

Message	Category	Explanation/Action
License expired	WARNING	The loaded (demo) license on the Nortel SNAS has expired. The Nortel SNAS now uses the default license.
Server <id> uses default interface (interface <n> not configured)	WARNING	A specific interface is configured to be used by the server but this interface is not configured on the Nortel SNAS.
IPSEC server <id> uses default interface (interface <n> not configured)	WARNING	A specific interface is configured to be used by the IPsec server but this interface is not configured on the Nortel SNAS.

Table 82 "Traffic Processing messages—INFO" (page 460) lists the Traffic Processing INFO messages.

Table 82
Traffic Processing messages—INFO

Message	Category	Explanation/Action
gzip error: <reason>	INFO	Problem encountered when processing compressed content.
gzip warning: <reason>	INFO	Problem encountered when processing compressed content.
accept() turned off (<nr>) too many fds	INFO	The Nortel SNAS has temporarily stopped accepting new connections. This happens when the Nortel SNAS is overloaded. The Nortel SNAS will start accepting connections once it has finished processing its current sessions.
No cert supplied by backend server	INFO	No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.
No CN supplied in server cert <subject>	INFO	No CN found in the subject of the certificate supplied by the backend server.
Bad CN supplied in server cert <subject>	INFO	Malformed CN found in subject of the certificate supplied by the backend server.
DNS alarm: dns server(s) are UP	INFO	At least one DNS server is now up.

Table 82
Traffic Processing messages—INFO (cont'd.)

Message	Category	Explanation/Action
HC: backend <ip>:<port> is down	INFO	Backend health check detected backend <ip>:<port> to be down.
HC: backend <ip>:<port> is up again	INFO	Backend health check detected backend <ip>:<port> to be up.

Start-up messages

The Traffic Processing Subsystem Start-up messages include the INFO category only.

Table 83 "Start-up messages—INFO" (page 461) lists the Start-up INFO messages.

Table 83
Start-up messages—INFO

Message	Category	Explanation/Action
Loaded <ip>:<port>	INFO	Initializing virtual server <ip>:<port>.
Since we use clicerts, force adjust totalcache size to : <size> per server that use clicerts	INFO	Generated if the size of the SSL session cache has been modified.
No TPS license limit	INFO	Unlimited TPS license used.
Found <size> meg of phys mem	INFO	Amount of physical memory found on system.

AAA subsystem messages

There are two categories of Authentication, Authorization, and Accounting (AAA) subsystem messages:

- ERROR (see Table 84 "AAA messages—ERROR" (page 461))
- INFO (see Table 85 "AAA messages—INFO" (page 462))

Table 84 "AAA messages—ERROR" (page 461) lists the AAA ERROR messages.

Table 84
AAA messages—ERROR

Message	Category	Explanation/Action
LDAP backend(s) unreachable Domain=\"<id>\" AuthId=\"<authid>\"	ERROR	Indicates LDAP server(s) cannot be reached when a user tries to log in to the portal.

Table 85 "AAA messages—INFO" (page 462) lists the AAA INFO messages. INFO messages are generated only if the CLI command **/cfg/domain #/adv/log** is enabled.

Table 85
AAA messages—INFO

Log value contains...	Message	Category	
login	NSNAS LoginSucceeded Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" Groups="<groups>"	INFO	Logon to the Nortel SNAS domain succeeded. The client's access method, IP address, user name, and group membership is shown.
	NSNAS LoginSucceeded Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"	INFO	Logon to the Nortel SNAS domain succeeded. The client's access method, IP address, user name and group membership is shown as well as the IP address allocated to the connection between the Nortel SNAS and the destination address (inner tunnel).
	NSNAS AddressAssigned Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"	INFO	Source IP address for the connection between the Nortel SNAS and the destination address (inner tunnel) has been allocated.
	NSNAS LoginFailed Domain="<id>" Method=<"ssl"> SrcIp="<ip>" [User="<user>"] Error=<error>	INFO	Logon to the Nortel SNAS domain failed. The client's access method, IP address, and user name is shown.
	NSNAS Logout Domain="<id>" SrcIp="<ip>" User="<user>"	INFO	The client's access method, IP address, has logged out from the Nortel SNAS domain.
portal	PORTAL Domain="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share> " Path="<path>"	INFO	The client has successfully accessed the specified folder/directory on the specified file server requested from the portal's Files tab.

Table 85
AAA messages—INFO (cont'd.)

Log value contains...	Message	Category	
http	HTTP Domain="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	The user has successfully accessed the specified web server requested from the portal.
	HTTP NotLoggedIn Domain="<id>" Host="<host>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	The user was not logged on to the specified web server requested from the portal.
reject	HTTP Rejected Domain="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	The client failed to access the specified web server requested from the portal.
	PORTAL Rejected Domain="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	The client failed to access the specified folder/directory on the specified file server requested from the portal's Files tab.
	SOCKS Rejected Domain="<id>" User="<user>" SrcIP="<ip>" Request="<request>"	INFO	The client failed to perform an operation by using one of the features available under the portal's Advanced tab.

NSNAS subsystem messages

There are two categories of NSNAS subsystem messages:

- ERROR (see Table 86 "NSNAS—ERROR" (page 463))
- INFO (see Table 87 "NSNAS—INFO" (page 464))

Table 86 "NSNAS—ERROR" (page 463) lists the NSNAS ERROR messages.

Table 86
NSNAS—ERROR

Message	Category	Explanation/Action
Domain:1, Switch: <switchID> ERROR cmd timeout for cmd :<commandID>	ERROR	An internal command between the specified switch and the Nortel SNAS timed out. Check connectivity between the switch and the Nortel SNAS.

Table 87 "NSNAS—INFO" (page 464) lists the NSNAS INFO messages.

Table 87
NSNAS—INFO

Message	Category	Explanation/Action
[A:B:C:D] NSNA portup	INFO	Domain A, switch B, unit C, port D Ethernet link is up.
[A:B:C:D] NSNA portdown	INFO	Domain A, switch B, unit C, port D Ethernet link is down.
LoginSucceeded Domain="1" SrcIp="<IPaddr>" Method="ssl" User= "<user>" Groups="<group>/<profile>/ "	INFO	On Domain 1, user "<user>" with IP : "<IP>" and belonging to group "<group>/<profile>/" has logged in.
transferring user <user> on Switch="1:<switchID>(<IPaddr>)", Port="<unit/port>" to Vlan="<vlan>(<vlanID>)"	INFO	Client device on Domain 1, Switch <switchID> (switch IP address <IPaddr>), Unit <unit>, Port <port> is being moved to the VLAN named <vlan> with VLAN ID <vlanID>.
switch controller:switch [1:<switchID>] – Modified	INFO	The CLI configuration of Domain 1, Switch <switchID> has been modified.
switch controller:switch [1:<switchID>] – Disconnected	INFO	Switch <switchID> of Domain 1 has disconnected from the NSNAS.
switch controller:switch [1:<switchID>] – Added	INFO	Switch <switchID> has been added to Domain 1.
switch controller:switch [1:<switchID>] - Deleted	INFO	Switch <switchID> has been deleted from Domain 1.
nhauser: user <username>[<pVIP>] – SRS check failed, restrictingSRS – <SRS rule> <comment> – <item> – <reason>	INFO	Nortel Health Agent applet report: The user with user name <username>, logged on to the Nortel SNAS portal with portal Virtual IP address <pVIP>, has failed the SRS rule check, and access is restricted in accordance with the behavior configured for SRS rule failure. To identify the rule, the message includes the <SRS rule> name and additional <comment> information defined for the rule. The message also includes the element of the SRS rule (<item>) that failed and the <reason> (for example, file not found).
nhauser: user <username>[<pVIP>] – SRS checks ok, open session	INFO	Nortel Health Agent applet report: The user with user name <username>, logged on to the Nortel SNAS portal with portal Virtual IP address <pVIP>, has passed the SRS rule check and is authorized to start a session in a Green VLAN.

Syslog messages in alphabetical order

Table 88 "Syslog messages in alphabetical order" (page 465) lists the syslog messages in alphabetical order.

Table 88
Syslog messages in alphabetical order

Message	Severity	Type	Explanation
[A:B:C:D] NSNA portdown	INFO	NSNAS	Domain A, switch B, unit C, port D Ethernet link is down.
[A:B:C:D] NSNA portup	INFO	NSNAS	Domain A, switch B, unit C, port D Ethernet link is up.
accept() turned off (<nr>) too many fds	INFO	Traffic Processing	The Nortel SNAS has temporarily stopped accepting new connections. This will happen when the Nortel SNAS is overloaded. It will start accepting connections once it has finished processing its current sessions.
Application filesystem corrupt - reinstall required	CRITICAL	OS	Reinstall.
audit	EVENT	System Control	Sent when a CLI system administrator enters, enters, exits or updates the CLI if audit logging is enabled using the **`/cfg/sys/adm/audit/ena`** command.
Bad CN supplied in server cert <subject>	INFO	Traffic Processing	Malformed CN found in subject of the certificate supplied by the backend server.
Bad IP:PORT data <line> in hc script	ERROR	Traffic Processing	Bad ip:port found in health check script. Please reconfigure the health script. This should normally be captured earlier by the CLI.
Bad regexp (<expr>) in health check	ERROR	Traffic Processing	Bad regular expression found in health check script. Please reconfigure. This should normally be captured earlier by the CLI.
Bad script op found <script op>	ERROR	Traffic Processing	Bad script operation found in health check script. Please reconfigure. This should normally be captured earlier by the CLI.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
Bad string found <string>	ERROR	Traffic Processing	Bad load balancing string encountered. This is normally verified by the CLI.
Can't bind to local address: <ip>:<port>: <reason>	ERROR	Traffic Processing	Problem encountered when trying to set up virtual server on <ip>:<port>.
Config filesystem corrupt	ERROR	OS	Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.
Config filesystem corrupt beyond repair	EMERG	OS	The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover.
Config filesystem re-initialized - reinstall required	CRITICAL	OS	Reinstall.
Config filesystem restored from backup	ERROR	OS	Loss of recent configuration changes.
Connect failed: <reason>	ERROR	Traffic Processing	Connect to backend server failed with <reason>.
copy_software_release_failed	ALARM (CRITICAL)	System Control	A Nortel SNAS failed to install a software release while trying to install the same version as all other Nortel SNAS devices in the cluster. The failing Nortel SNAS tries to catch up with the other cluster members as it was not up and running when the new software version was installed.
css error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an style sheet. It may be a problem with the css parser in the Nortel SNAS or it could be a problem on the processed page.
DNS alarm: all dns servers are DOWN	CRITICAL	Traffic Processing	All DNS servers are down. The Nortel SNAS cannot perform any DNS lookups.
DNS alarm: dns server(s) are UP	INFO	Traffic Processing	At least one DNS server is now up.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
Domain:1, Switch: <switchID> ERROR cmd timeout for cmd :<commandID>	ERROR	NSNAS	An internal command between the specified switch and the Nortel SNAS timed out. Check connectivity between the switch and the Nortel SNAS.
failed to locate corresponding portal for portal authenticated http server	ERROR	Traffic Processing	Portal authentication has been configured for an http server, but no portal using the same xnet domain can be found. Make sure that there is a portal running using the same xnet id.
Failed to log to CLI :<reason> -- disabling CLI log	ERROR	Traffic Processing	Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.
failed to parse Set-Cookie <header>	ERROR	Traffic Processing	The Nortel SNAS got a malformed Set-Cookie header from the backend web server.
Failed to syslog traffic :<reason> -- disabling traf log	ERROR	Traffic Processing	Problem occurred when the Nortel SNAS tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.
Failed to write to config filesystem	EMERG	OS	Probable hardware error. Reinstall.
Found <size> meg of phys mem	INFO	Start-up	Amount of physical memory found on system.
gzip error: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
gzip warning: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
HC: backend <ip>:<port> is down	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be down.
HC: backend <ip>:<port> is up again	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be up.
html error: <reason>	ERROR	Traffic Processing	Error encountered when parsing HTML. Probably non-standard HTML.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
http error: <reason>, Request="<method> <host><path>"	ERROR	Traffic Processing	A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the Nortel SNAS 's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.
http header warning cli: <reason> (<header>)	ERROR	Traffic Processing	The client sent a bad HTTP header.
http header warning srv: <reason> (<header>)	ERROR	Traffic Processing	The server sent a bad HTTP header.
HTTP NotLoggedIn Domain="<id>" Host="<host>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The user was not logged on to the specified web server requested from the Portal.
HTTP Rejected Domain="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The user failed to access the specified web server requested from the Portal.
HTTP Domain="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The user has successfully accessed the specified web server requested from the Portal.
Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>	ERROR	Traffic Processing	Nortel SNAS received reply for non-configured DNS server.
internal error: <no>	ERROR	Traffic Processing	An internal error occurred. Please contact support with as much information as possible to reproduce this message.
IPSEC server <id> uses default interface (interface <n> not configured)	WARNING	Traffic Processing	A specific interface is configured to be used by the IPsec server but this interface is not configured on the Nortel SNAS.
isd_down	ALARM (CRITICAL)	System Control	A member of the Nortel SNAS cluster is down. This alarm is only sent if the cluster contains more than one Nortel SNAS.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
javascript error: <reason> for: <host><path>	ERROR	Traffic Processing	JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the Nortel SNAS JavaScript parser, but most likely a syntactical error in the JavaScript on that page.
jscript.encode error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the Nortel SNAS or it could be a problem on the processed page.
LDAP backend(s) unreachable Domain=\"<id>\" AuthId=\"<authid>\"	ERROR	AAA	Shown if LDAP server(s) cannot be reached when a user tries to login to the Portal.
license	ALARM (WARNING)	System Control	One or several Nortel SNAS devices in the cluster do not have the same SSL Nortel SNAS license (with reference to number of concurrent users).
license	ALARM (WARNING)	System Control	The (demo) license loaded to the local Nortel SNAS expires within 7 days. Check loaded licenses using the **`/cfg/sys/cur`** command.
license_expired	EVENT	System Control	Indicates that the the demo license at host <IP> has expired. Check the loaded licenses with **`/cfg/sys/cur`**.
License expired	WARNING	Traffic Processing	The loaded (demo) license on the Nortel SNAS has expired. The Nortel SNAS now uses the default license.
Loaded <ip>:<port>	INFO	Start-up	Initializing virtual server <ip>:<port>.
log_open_failed	ALARM (MAJOR)	System Control	The event log (where all events and alarms are stored) could not be opened.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
LoginSucceeded Domain="1" SrcIp="<IPaddr>" Method="ssl" User="<user>" Groups="<group>/<profile>/	INFO	NSNAS	On Domain 1, user "<user>" with IP : "<IP>" and belonging to group "<group>/<profile>/" has logged in.
Logs filesystem re-initialized	ERROR	OS	Loss of logs.
make_software_release_permanent_failed	ALARM (CRITICAL)	System Control	Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.
Missing files in config filesystem	ERROR	OS	Possible loss of configuration. Followed by the message "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup".
No cert supplied by backend server	INFO	Traffic Processing	No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.
No CN supplied in server cert <subject>	INFO	Traffic Processing	No CN found in the subject of the certificate supplied by the backend server.
No more than <nr> backend supported	INFO	Start-up	Generated when more than the maximum allowed backend servers have been configured.
No PortalGuard license loaded: Domain <id> *will* use portal authentication	WARNING	Traffic Processing	The PortalGuard license has not been loaded on the Nortel SNAS.
No Secure Service Partitioning loaded: server <id> *will not* use interface <n>	WARNING	Traffic Processing	The Secure Service Partitioning license has not been loaded on the Nortel SNAS but the server is configured to use a specific interface.
No TPS license limit	INFO	Start-up	Unlimited TPS license used.
NSNAS AddressAssigned Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"	INFO	AAA	Source IP address for the connection between the Nortel SNAS and the destination address (inner tunnel) has been allocated.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
NSNAS LoginFailed Domain="<id>" Method=<"ssl"> SrcIp="<ip>" [User="<user>"] Error=<error>	INFO	AAA	Logon to the Nortel SNAS domain failed. The client's access method, IP address, and user name is shown.
NSNAS LoginSucceeded Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" Groups="<groups>"	INFO	AAA	Login to the Nortel SNAS domain succeeded. The client's access method, IP address, user name and group membership is shown.
NSNAS LoginSucceeded Domain="<id>" Method=<"ssl"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"	INFO	AAA	Login to the Nortel SNAS domain succeeded. The client's access method, client IP address, user name and group membership is shown as well as the IP address allocated to the connection between the Nortel SNAS and the destination address (inner tunnel).
NSNAS Logout Domain="<id>" SrcIp="<ip>" User="<user>"	INFO	AAA	Client has logged out from the Nortel SNAS domain.
partitioned_network	EVENT	System Control	Sent to indicate that a Nortel SNAS is recovering from a partitioned network situation.
PORTAL Rejected Domain="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user failed to access the specified folder/directory on the specified file server requested from the Portal's Files tab.
PORTAL Domain="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user has successfully accessed the specified folder/directory on the specified file server requested from the Portal's Files tab.
Rebooting to revert to permanent OS version	ERROR	OS	Happens after "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup" if software upgrade is in progress (i.e. if failure at first boot on new OS version).
reload cert config done	INFO	Config Reload	Certificate reloading done.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
reload cert config start	INFO	Config Reload	Starting reloading of certificates.
reload configuration done	INFO	Config Reload	Virtual server configuration reloading done.
reload configuration network down	INFO	Config Reload	Accepting new sessions are temporarily put on hold.
reload configuration network up	INFO	Config Reload	Resuming accepting new sessions after loading new configuration.
reload configuration start	INFO	Config Reload	Virtual server configuration reloading start.
Root filesystem corrupt	EMERG	OS	The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover.
Root filesystem repaired - rebooting	ERROR	OS	fsck found and fixed errors. Probably OK.
Server <id> uses default interface (interface <n> not configured)	WARNING	Traffic Processing	A specific interface is configured to be used by the server but this interface is not configured on the Nortel SNAS.
Set CSWIFT as default	INFO	Start-up	Using CSWIFT SSL hardware acceleration.
Since we use clicerts, force adjust totalcache size to : <size> per server that use clicerts	INFO	Start-up	Generated if the size of the SSL session cache has been modified.
single_master	ALARM (WARNING)	System Control	Only one master Nortel SNAS in the cluster is up and running.
socks error: <reason>	ERROR	Traffic Processing	Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.
SOCKS Rejected Domain="<id>" User="<user>" SrcIP="<ip>" Request="<request>"	INFO	AAA	The client failed to perform an operation by using one of the features available under the portal's Advanced tab.
socks request: socks version <version> rejected	ERROR	Traffic Processing	Socks request of version <version> received and rejected. Most likely a non-standard socks client.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
SOCKS Domain="<id>" User="<user>" SrcIP="<ip>" Request="<request>"	INFO	AAA	The client has successfully performed an operation by using one of the features available under the portal's Advanced tab.
software_configuration_changed	EVENT	System Control	Indicates that release <VSN> (version) has been <Status> (unpacked/installed/permanent).
software_release_copying	EVENT	System Control	Indicates that <IP> is copying the release <VSN> from another cluster member.
software_release_rebooting	EVENT	System Control	Indicates that a Nortel SNAS (<IP>) is rebooting on a new release (in other words, a Nortel SNAS that was not up and running during the normal installation is now catching up).
ssi_mipishere	EVENT	System Control	Tells that the MIP (management IP address) is now located at the Nortel SNAS with the <IP> host IP address.
switch controller:switch [1:<switchID>] – Added	INFO	NSNAS	Switch <switchID> has been added to Domain 1.
switch controller:switch [1:<switchID>] - Deleted	INFO	NSNAS	Switch <switchID> has been deleted from Domain 1.
switch controller:switch [1:<switchID>] – Disconnected	INFO	NSNAS	Switch <switchID> of Domain 1 has disconnected from the NSNAS.
switch controller:switch [1:<switchID>] – Modified	INFO	NSNAS	The CLI configuration of Domain 1, Switch <switchID> has been modified.
System started [isdssl-<version>]	INFO	System Control	Sent whenever the system control process has been (re)started.
The private key and certificate don't match for <server nr>	ERROR	Traffic Processing	Key and certificate does not match for server #. The certificate has to be changed.
TPS license limit (<limit>) exceeded	WARNING	Traffic Processing	The transactions per second (TPS) limit has been exceeded.
TPS license limit: <limit>	INFO	Start-up	TPS limit set to <limit>.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
transferring user <user> on Switch="1:<switchID>(<IPaddr>)", Port="<unit/port>" to Vlan="<vlan>(<vlanID>)	INFO	NSNAS	Client device on Domain 1, Switch <switchID> (switch IP address <IPaddr>), Unit <unit>, Port <port> is being moved to the VLAN named <vlan> with VLAN ID <vlanID>.
nhauser: user <username>[<pVIP>] – SRS check failed, restrictingSRS – <SRS rule> <comment> – <item> – <reason>	INFO	NSNAS	Nortel Health Agent applet report: The user with user name <username>, logged on to the Nortel SNAS portal with portal Virtual IP address <pVIP>, has failed the SRS rule check, and access is restricted in accordance with the behavior configured for SRS rule failure. To identify the rule, the message includes the <SRS rule> name and additional <comment> information defined for the rule. The message also includes the element of the SRS rule (<item>) that failed and the <reason> (for example, file not found).
nhauser: user <username>[<pVIP>] – SRS checks ok, open session	INFO	NSNAS	Nortel Health Agent applet report: The user with user name <username>, logged on to the Nortel SNAS portal with portal Virtual IP address <pVIP>, has passed the SRS rule check and is authorized to start a session in a Green VLAN.
Unable to find client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Please reconfigure.
Unable to use client certificate for <server #>	ERROR	Traffic Processing	Certificate for doing sslconnect is not valid. Please reconfigure.
Unable to use client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Please reconfigure.
Unable to use the certificate for <server nr>	ERROR	Traffic Processing	Unsuitable certificate configured for server #.
unknown WWW-Authenticate method, closing	ERROR	Traffic Processing	Backend server sent unknown HTTP authentication method.

Table 88
Syslog messages in alphabetical order (cont'd.)

Message	Severity	Type	Explanation
vbscript error: <reason> for: <host><path>	ERROR	Traffic Processing	VBScript parsing error encountered when parsing content from <host><path>. This could be a problem in the Nortel SNAS VBScript parser, but most likely a syntactical error in the VBScript on that page.
www_authenticate: bad credentials	ERROR	Traffic Processing	The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

Appendix Supported MIBs

This appendix describes the Management Information Bases (MIB) and traps supported by the Nortel SNAS.

- “Supported MIBs” (page 477)
- “Supported traps” (page 481)

For detailed information about the MIB definitions currently implemented for the SNMP agent, do the following:

Step	Action
1	Go to http://www.nortel.com/support.
2	Navigate to the Nortel SNAS Software page.
3	Download the tar.gz file for the Nortel SNAS MIBs.
4	Unzip the .tar file in order to access the file ALTEON-SAC-CAP.mib. ALTEON-SAC-CAP.mib contains an AGENT-CAPABILITIES statement, which formally specifies which MIBs are implemented.

--End--

For information about configuring the SNMP agent in a cluster, see “Configuring SNMP” (page 323).

Supported MIBs

The following MIBs are supported by the Nortel SNAS:

- ALTEON-ISD-PLATFORM-MIB
- ALTEON-ISD-SSL-MIB
- ALTEON-ROOT-MIB

- ALTEON-SAC-CAP
- ALTEON-SSL-VPN-MIB
- ANAifType-MIB
- DISMAN-EVENT-MIB
- ENTITY-MIB
- IF-MIB
- IP-FORWARD-MIB
- IP-MIB
- NORTEL-SECURE-ACCESS-SWITCH-MIB
- S5-ROOT-MIB
- S5-TCS-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USER-BASED-SM-MIB
- SNMPv2-MIB
- SNMP-VIEW-BASED-ACM-MIB
- SYNOPTICS-ROOT-MIB
- 5-ETH-MULTISEG-TOPOLOGY-MIB

Table 89 "Supported MIBs" (page 478) provides more information about some of the MIBs supported by the Nortel SNAS.

Table 89
Supported MIBs

MIB	Description
ALTEON-ISD-PLATFORM-MIB	Contains the following groups and objects: • isdClusterGroup • isdResourceGroup • isdAlarmGroup • isdBasicNotificatioObjectsGroup • isdEventNotificationGroup • isdAlarmNotificationGroup

Table 89
Supported MIBs (cont'd.)

MIB	Description
ALTEON-ISD-SSL-MIB	Contains objects for monitoring the SSL gateways. The following groups are implemented: • sslBasicGroup • sslEventGroup
ALTEON-SSL-VPN-MIB	The following group is implemented: • vpnBasicGroup
DISMAN-EVENT-MIB	The MIB module for defining event triggers and actions. The following groups are implemented: • dismanEventResourceGroup • dismanEventTriggerGroup • dismanEventObjectsGroup • dismanEventEventGroup • dismanEventNotificationObjectGroup
ENTITY-MIB	The following groups are implemented: • entityPhysicalGroup • entityPhysical2Group • entityGeneralGroup • entityNotificationsGroup Write access to snmpTargetParamsTable is turned off in VACM.
IF-MIB	The following groups are implemented: • ifPacketGroup • ifStackGroup **Limitations** The agent does not implement the following objects: • ifType • ifSpeed • ifLastChange

Table 89
Supported MIBs (cont'd.)

MIB	Description
	• ifInUnknownProtos • ifOutNUnicast
IP-FORWARD-MIB	The following group is implemented: • ipCidrRouteGroup
IP-MIB	The following groups are implemented: • ipGroup • icmpGroup
NORTEL-SECURE-ACCESS-SWITCH-MIB	Contains objects for monitoring the Nortel SNAS devices. The following groups are implemented: • snasBasicGroup • snasEventGroup
SNMP-FRAMEWORK-MIB	The following group is implemented: • snmpEngineGroup
SNMP-MPD-MIB	The following group is implemented: • snmpMPDGroup
SNMP-NOTIFICATION-MIB	The following group is implemented: • snmpNotifyGroup Write access to all objects in this MIB is turned off in VACM.
SNMP-TARGET-MIB	The SNMP-TARGET-MIB contains information about where to send traps. You can configure and view trap information from the CLI, using the **`/cfg/sys/adm/snmp/target`** command (see "Configuring SNMP notification targets" (page 331)). The following groups are implemented: • snmpTargetCommandResponderGroup • snmpTargetBasicGroup • snmpTargetResponseGroup Write access to snmpTargetParamsTable is turned off in VACM.

Table 89
Supported MIBs (cont'd.)

MIB	Description
SNMP-USER-BASED-SM-MIB	The following group is implemented: • usmMIBBasicGroup Write access to all objects in this MIB is turned off in VACM.
SNMPv2-MIB	A standard MIB implemented by all agents. The following groups are implemented: • snmpGroup • snmpSetGroup • systemGroup • snmpBasicNotificationsGroup • snmpCommunityGroup
SNMP-VIEW-BASED-ACM-MIB	The following group is implemented: • vacmBasicGroup Write access to all objects in this MIB is turned off in VACM.

Supported traps

Table 90 "Supported traps" (page 481) describes the traps supported by the Nortel SNAS.

Table 90
Supported traps

Trap Name	Description
authenticationFailure	Sent when the SNMP agent receives an SNMP message which is not properly authenticated. This trap is disabled by default. To enable the trap through SNMP, set **snmpEnableAuthenTraps** to enabled or use the CLI command **/cfg/sys/adm/snmp/snmpv2-mib/snmpenable**. Defined in SNMPv2-MIB.
coldStart	Sent when the Nortel SNAS reboots. Defined in SNMPv2-MIB.
isdAlarmCleared	Sent when an alarm is cleared.

Table 90
Supported traps (cont'd.)

Trap Name	Description
isdDown	Signifies that a Nortel SNAS device in the cluster is down and out of service.
isdLicense	Sent when the Nortel SNAS devices in the cluster have different licenses and when a demo license has seven days left before expiration. Defined in ALTEON-ISD-PLATFORM-MIB.
isdLicenseExpired	Sent when a license has expired.
isdMipMigration	Signals that the master IP has migrated to another Nortel SNAS.
isdSingleMaster	Signifies that only one master Nortel SNAS in the cluster is up and operational. Only having one master in a cluster means that the fault tolerance level is severely degraded—if the last master fails, the system cannot be reconfigured.
linkDown	Sent when the agent detects that one of the links (interfaces) has gone down. Defined in IF-MIB.
linkUp	Sent when the agent detects that one of the links (interfaces) has gone up. Defined in IF-MIB.

Appendix Supported ciphers

The Nortel SNAS supports SSL version 2.0, SSL version 3.0, and TLS version 1.0. The Nortel SNAS supports all ciphers covered in these versions of SSL, except the IDEA and FORTEZZA ciphers and ciphers using DH or DSS authentication.

Table 91
Supported ciphers

Cipher name	SSL protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
DHE-RSA-AES256-SHA	SSLv3	DH, RSA	AES (256)	SHA1
AES256-SHA	SSLv3	RSA, RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	DH, RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSLv3	RSA, RSA	3DES (168)	SHA1
DES-CBC3-MD5	SSLv2	RSA, RSA	3DES (168)	MD5
DHE-RSA-AES128-SHA	SSLv3	DH, RSA	AES (128)	SHA1
AES128-SHA	SSLv3	RSA, RSA	AES (128)	SHA1
RC4-SHA	SSLv3	RSA, RSA	RC4 (128)	SHA1
RC4-MD5	SSLv3	RSA, RSA	RC4 (128)	MD5
RC2-CBC-MD5	SSLv2	RSA, RSA	RC2 (128)	MD5
RC4-MD5	SSLv2	RSA, RSA	RC4 (128)	MD5
RC4-64-MD5	SSLv2	RSA, RSA	RC4 (64)	MD5
EXP1024-RC4-SHA	SSLv3	RSA(1024), RSA	RC4 (56)	SHA1 EXPORT
EXP1024-DES-CBC-SHA	SSLv3	RSA (1024), RSA	DES (56)	SHA1 EXPORT
EXP1024-RC2-CBC-MD5	SSLv3	RSA (1024), RSA	RC2 (56)	MD5 EXPORT

Table 91
Supported ciphers (cont'd.)

Cipher name	SSL protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
EXP1024-RC4-MD5	SSLv3	RSA (1024), RSA	RC4 (56)	MD5 EXPORT
EDH-RSA-DES-CBC-SHA	SSLv3	DH, RSA	DES (56)	SHA1
DES-CBC-SHA	SSLv3	RSA, RSA	DES (56)	SHA1
DES-CBC-MD5	SSLv2	RSA, RSA	DES (56)	MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512), RSA	DES (40)	SHA1 EXPORT
EXP-DES-CBC-SHA	SSLv3	RSA (512), RSA	DES (40)	SHA1 EXPORT
EXP-RC2-CBC-MD5	SSLv3	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv3	RSA (512), RSA	RC4 (40)	MD5 EXPORT
EXP-RC2-CBC-MD5	SSLv2	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv2	RSA (512), RSA	RC4 (40)	MD5 EXPORT
ADH-AES256-SHA	SSLv3	DH, NONE	AES (256)	SHA1
ADH-DES-CBC3-SHA	SSLv3	DH, NONE	3DES (168)	SHA1
ADH-AES128-SHA	SSLv3	DH, NONE	AES (128)	SHA1
ADH-RC4-MD5	SSLv3	DH, None	RC4 (128)	MD5
ADH-DES-CBC-SHA	SSLv3	DH, NONE	DES (56)	SHA1
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512), None	DES (40)	SHA1 EXPORT
EXP-ADH-RC4-MD5	SSLv3	DH (512), None	RC4 (40)	MD5 EXPORT

Appendix Adding User Preferences attribute to Active Directory

For the remote user to be able to store user preferences on the Nortel SNAS, you need to add the *isdUserPrefs* attribute to Active Directory. This attribute will contain an opaque data structure, containing various information that the user may have saved during a Portal session.

This description is based on Windows 2000 Server and Windows Server 2003. Make sure that your account is a member of the Schema Administrators group.

Install All Administrative Tools (Windows 2000 Server)

Step	Action
1	Open the Control Panel and double-click Add/Remove Programs.
2	Select Windows 2000 Administrative Tools and click Change.
3	Click Next and select Install All Administrative Tools.
4	Follow the instructions on how to proceed with the installation.

--End--

Register the Schema Management dll (Windows Server 2003)

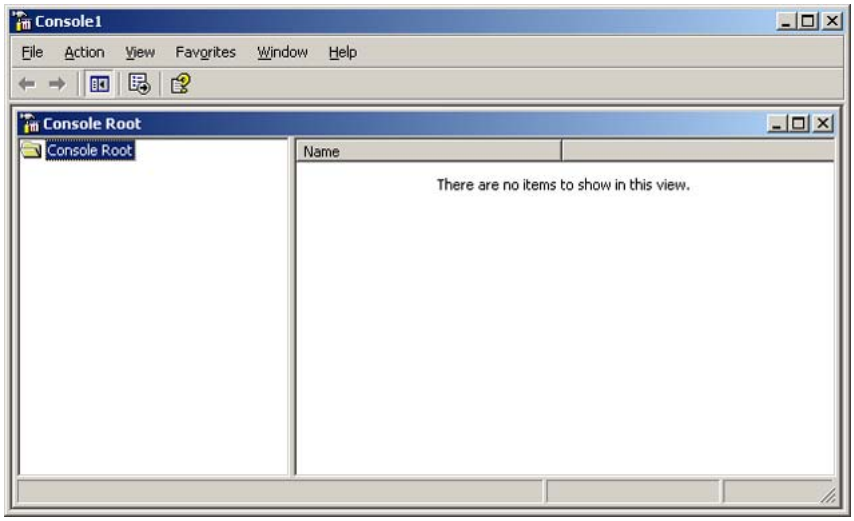
Step	Action
1	Click Start and select Run.
2	In the Open field, enter **`regsvr32 schmmgmt.dll`**. Note that there is a space between regsvr32 and schmmgmt.dll.
3	Click OK.

This command will register schmmgmt.dll on your computer.

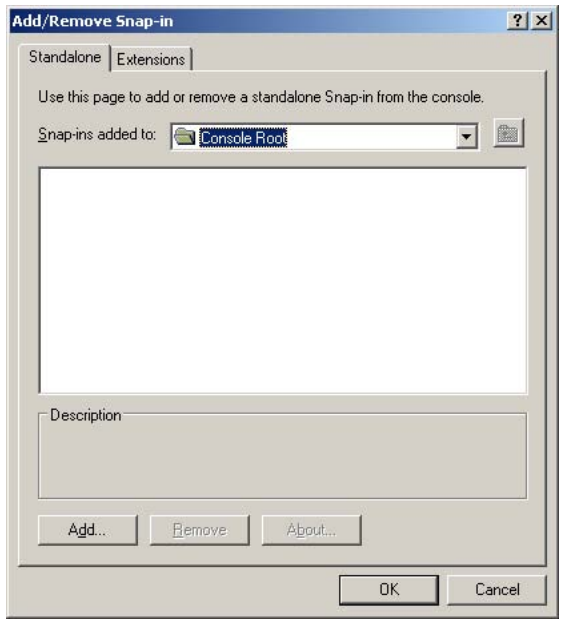
--End--

Add the Active Directory Schema Snap-in (Windows 2000 Server and Windows Server 2003)

Step	Action
1	Click Start and select Run.
2	On Windows 2000 Server, enter **mmc** in the Open field. On Windows Server 2003, enter **mmc /a** instead. Note that there is a space between **mmc** and **/a**.
3	Click OK. The Console window .

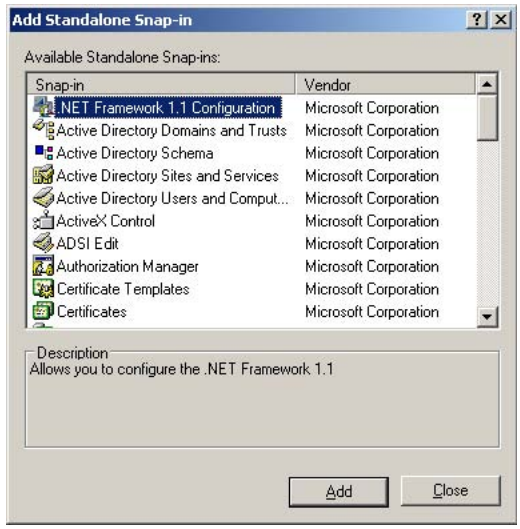


4	On the File (Console) menu, select Add/Remove Snap-in. The Add/Remove Snap-in window .



5 Click **Add**.

The Add Standalone Snap-in window appears.



6 Under Snap-in, select Active Directory Schema and click **Add**.

Active Directory Schema is added to the Add/Remove Snap-in window.

7 Click **Close**to close the Add Standalone Snap-in window.

8 Click **OK**.

The Console window appears.

9	To save the console (including the Schema snap-in), go to the File (Console) menu and select Save. The Save As windows appears.
10	Save the console in the Windows\System 32 root folder. Give the file name, as **`schmmgmt.msc`**.
11	Click **Save**.

--End--

Create a shortcut to the console window

Step	Action
1	Right-click Start, and select Open all Users.
2	Double-click the Programs and Administrative Tools folders.
3	On the File menu, point to New, and then select Shortcut. The Create Shortcut Wizard appears.
4	In the Type the location of the item field, type **`schmmgmt.msc`**.
5	Click **Next**. The **Select a Title for the Program** page appears.
6	In the Type a name for this shortcut field, type **`Active Directory Schema`**.
7	Click **Finish**.

--End--

Permit write operations to the schema (Windows 2000 Server)

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

Step	Action
1	In the Console window, on the left pane, right-click Active Directory Schema.
2	Select Operations Master.
3	Select the check box, the Schema may be modified on this Domain Controller.

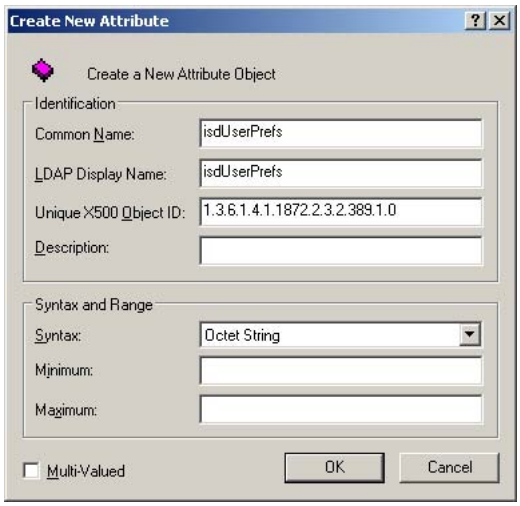
4 Click **OK**.

--End--

Create a new attribute (Windows 2000 Server and Windows Server 2003)

To create the *isdUserPrefs* attribute, proceed as follows:

Step	Action
1	In the Console window, on the left pane, expand Active Directory Schema by clicking the plus (+) sign. The Attributes and Classes folders display.
2	Right-click Attributes, point to New and select Attribute. You receive a warning that creating schema objects is a permanent operation and cannot be undone.
3	Click **Continue**. The Create New Attribute window appears.
4	Create the isdUserPrefs attribute as shown below:



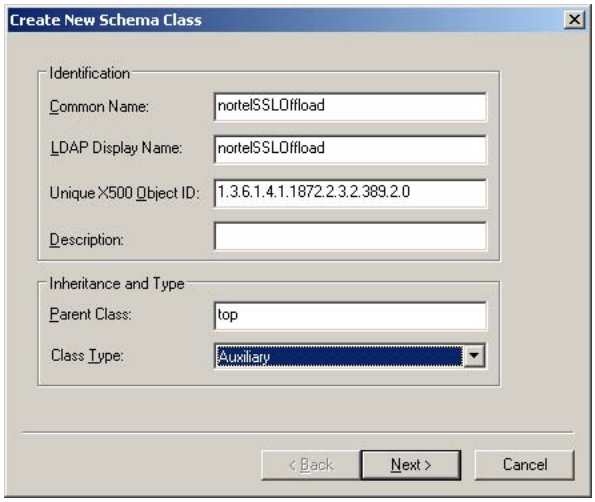
5 Click **OK**.

--End--

Create the new class

To create the *nortelSSLOffload* class, proceed as follows:

Step	Action
1	In the Console window, right-click Classes, point to New and select Class. You will now receive a warning that creating schema classes is a permanent operation and cannot be undone.
2	Click Continue. The Create New Schema Class window appears.
3	Create the nortelSSLOffload class as shown below:

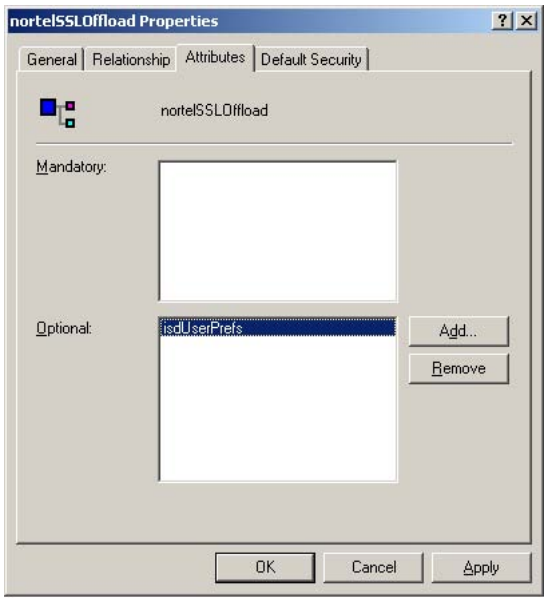


4	Click **OK**.

--End--

Add isdUserPrefs attribute to nortelSSLOffload class

Step	Action
1	In the Console window, on the left pane, expand Classes.
2	Select the nortelSSLOffload class.
3	Right-click and select Properties. The Properties window appears.
4	Select the Attributes tab and click **Add**.
5	Add the isdUserPrefs attribute as optional.



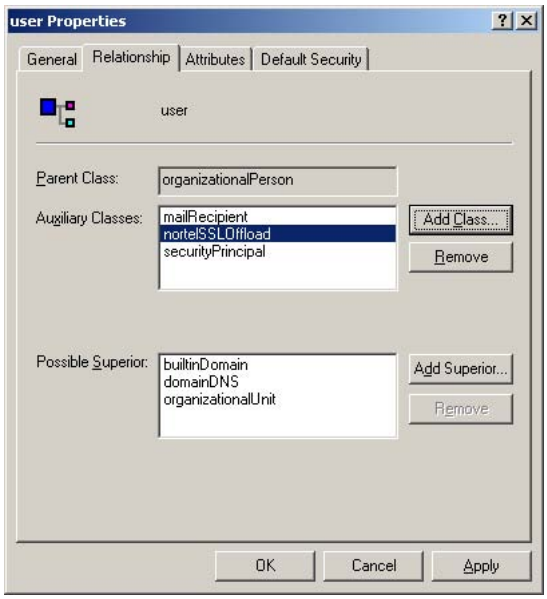
6 On the Default Security (Security) tab, set read/write permissions for the group that should have permission to write user preferences to the attribute.

7 Click **OK**.

--End--

Add the nortelSSLOffload Class to the User Class

Step	Action
1	In the Console window, on the left pane, expand Classes and select user.
2	Right-click and select Properties. The Properties window is displayed.
3	Select the Relationship tab.
4	Next to Auxiliary Classes, click Add Class (Add).
5	Add the nortelSSLOffload class as an auxiliary class as shown below:



6 Click OK.

Once you have enabled the User Preferences feature on the Nortel SNAS (using the CLI command **`/cfg/domain #/aaa/auth #/ldap/enauserpre`** or the BBI setting User Preferences under **VPN Gateways>Authentication>Auth Servers (LDAP)>Modify**) the remote user should now be able to store user preferences in Active Directory.

--End--

Appendix Configuring DHCP to auto-configure IP Phones

The DHCP server and the IP Phone 2002, IP Phone 2004, and IP Phone 2007 can be configured so that the IP Phone automatically obtains its configuration data from the DHCP server. This feature reduces the administrative overhead associated with bringing a large number of IP Phones online.

In addition, the DHCP server and the IP Phone can be configured so that the IP Phone can use the Auto VLAN Discovery feature, which allows the IP Phone to discover the Phone VLAN ID.

This appendix explains how to:

- configure the IP Phone to obtain its configuration data from a Windows 2000 Server DHCP server
- retrieve VLAN information required to take advantage of the Auto VLAN Discovery feature

This appendix is not intended to be a primer on how to set up a DHCP server. The reader is assumed to have a working knowledge of Windows 2000 Server DHCP servers. The appendix also does not describe the process used by the IP Phone to interact with the DHCP server or to boot itself into the Phone VLAN.

ATTENTION
It is assumed that the necessary DHCP scopes defining the range of addresses and lease duration have been created.

To take advantage of the Auto VLAN Discovery feature, two VLANs are required: one for the phone to boot into initially, in order to communicate with the DHCP server and learn the appropriate phone VLAN ID, and the second for the Phone VLAN itself.

For information on the minimum firmware versions required to support IP Phones in the Nortel SNAS, see *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.6.1 (NN47230-400)*, .

Configuring IP Phone auto-configuration

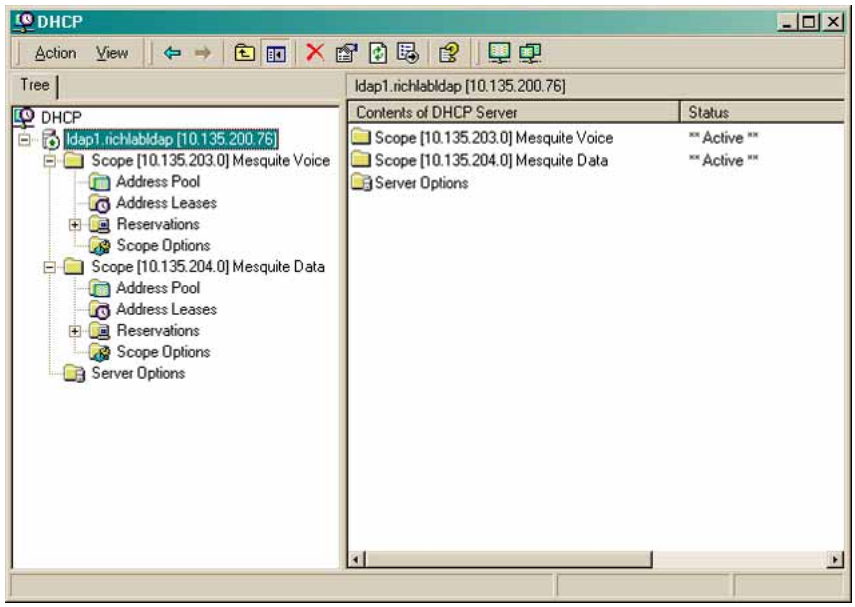
To configure Windows 2000 Server DHCP to auto-configure the IP Phones, perform the following steps:

Step	Action
1	Create DHCP options (see “Creating the DHCP options” (page 494)) • Call Server Information • VLAN Information for auto-discovery of the IP Phone VLAN ID
2	Configure the DHCP options (see “Configuring the Call Server Information and VLAN Information options” (page 497)) Repeat this step for the data (or boot) VLAN and the Phone VLAN.
3	Set up the IP Phone (see “Setting up the IP Phone” (page 500))
	--End--

Creating the DHCP options

Step	Action
1	On the Windows 2000 Server Start menu, select **Programs > Administrative Tools > DHCP**. The DHCP Management Console opens (see Figure 33 "The DHCP Management Console" (page 495)).

Figure 33
The DHCP Management Console



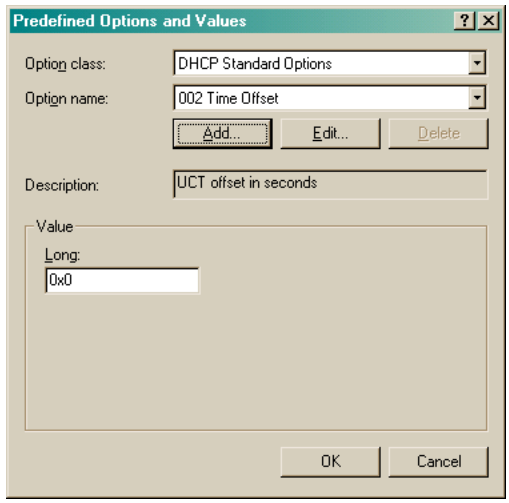
2 Select the DHCP server you want to configure.

ATTENTION
When you expand the DHCP server navigation tree component, the scopes for that particular server are listed below the server name and IP address.

3 From the DHCP Management Console toolbar, select **Action > Set Predefined Options**.

The Predefined Options and Values dialog box opens (see Figure 34 "The Predefined Options and Values dialog box" (page 496)).

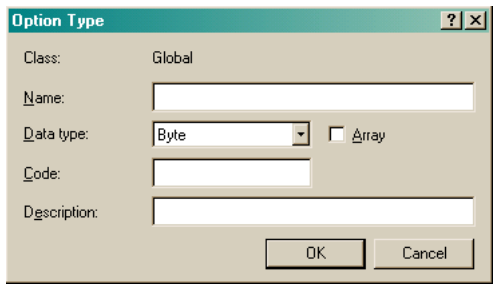
Figure 34
The Predefined Options and Values dialog box



4 Click **Add**.

The Option Type dialog box opens (see Figure 35 "The Option Type dialog box" (page 496)).

Figure 35
The Option Type dialog box



5 Create the DHCP option for the call server information.

a In the Option Type dialog box, enter the required information (see Table 92 "Option Type dialog box field values for Call Server Information" (page 496)).

Table 92
Option Type dialog box field values for Call Server Information

Field	Value
Name	Call Server Information
Data type	String
Code	128 (Call Server configuration)
Description	Comments (Optional)

b Click **OK**.

6 Create the DHCP option for the auto-discovery of VLAN ID information:

a In the Predefined Options and Values dialog box, click **Add**.

The Option Type dialog box opens (see Figure 35 "The Option Type dialog box" (page 496)).

b In the Option Type dialog box, enter the required information (see Table 93 "Option Type dialog box field values for VLAN Information" (page 497)).

Table 93
Option Type dialog box field values for VLAN Information

Field	Value
Name	VLAN Information
Data type	String
Code	191
Description	Comments (Optional)

c Click **OK**.

7 In the Predefined Options and Values dialog box, click **OK**, to return to the DCHP Management Console.

--End--

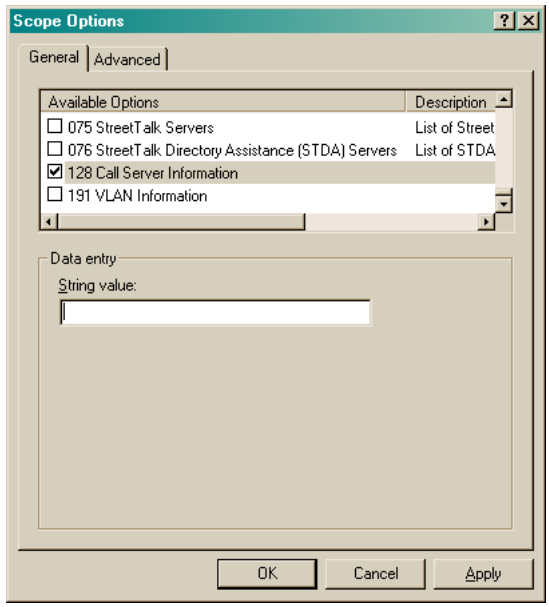
Configuring the Call Server Information and VLAN Information options

For the Auto VLAN Discovery feature, you must configure the options for both the data (or boot) VLAN and the Phone VLAN. Configure the option for the data (or boot) VLAN first, then repeat the steps to configure the option for the Phone VLAN.

To configure the options, perform the following steps.

Step	Action
1	In the DHCP Management Console, expand the required VLAN: • first, the data (or boot) VLAN used with the IP Phone • when you repeat the steps, the Phone VLAN
2	Right-click Scope Options, and select **Configure Options**. The Scope Options dialog box (see Figure 36 "The Scope Options dialog box" (page 498)).

Figure 36
The Scope Options dialog box



3 Using the scroll bar, scroll down the list to find the two DHCP options just created.

4 Configure Call Server Information:

a Select the check box beside 128 Call Server Information.

b In the String value field, enter the following string:

Nortel-i2004-A,iii.iii.iii.iii:ppppp,aaa,rrr;iii.iii.iii.iii:ppppp,aaa,rrr.

ATTENTION
The Nortel IP Phone 2002, IP Phone 2004, and IP Phone 2007 use the same signature. Therefore, the string value for Call Server Information is the same for all these IP Phones.

Table 94 "Call Server Information string parameter values" (page 498) describes the parameters.

Table 94
Call Server Information string parameter values

Parameter	Description
A	The hardware revision of the IP Phone
iii.iii.iii.iii	The IP Address of the Call Server (S1 or S2)
ppppp	The port number for the Call Server

Table 94
Call Server Information string parameter values (cont'd.)

Parameter	Description
aaa	The Action for the server
rrr	The Retry Count for the server

The DHCP Option #128 pertains to the Call Server information that the IP Phone will need in order to connect to the call server.

The following rules apply:

- The IP Address must be separated from the port by a colon (:).
- The parameters for the Primary (S1) and Secondary (S2) are separated by a semicolon (;).
- The string must end in a period (.)

ATTENTION
After you have entered the string, it will subsequently appear automatically each time the option is added to a scope.

c Click **Apply**.

5 Configure VLAN Information:

a In the Scope Options dialog box (see Figure 36 "The Scope Options dialog box" (page 498)), select 191 VLAN Information.

b In the String value field, enter the following string:

VLAN-A:vvvv.

Table 95 "VLAN ID Information string parameter values" (page 499) describes the parameters.

Table 95
VLAN ID Information string parameter values

Parameter	Description
A	The hardware revision of the IP Phone
vvvv	The VLAN ID in decimal

The site-specific option #191 pertains to the VLAN ID information that the IP Phone will require in order to boot into the Phone VLAN.

The following rules apply:

- A colon (:) separates the hardware revision from the VLAN ID.
- The string must end in a period (.)

c Click **Apply**

6 Click **OK**.

7 Repeat step 1 through step 6 to configure the options for the Phone VLAN.

--End--

Setting up the IP Phone

In order for the IP Phone to take advantage of the DHCP auto-configuratio n features, set the IP Phone up as follows:

Step	Action
1	Set the DHCP Option on the IP Phone to `1` to use DHCP.
2	Select `0` to set the phone to use FULL DHCP.
3	Select `2` (for `Automatic`) to set the phone to learn its VLAN ID from the DHCP server.

--End--

Appendix Using a Windows domain logon script to launch the Nortel SNAS portal

This appendix explains how to configure a Windows domain logon script to automatically launch an end user's browser on startup and present the Nortel SNAS portal page.

This appendix includes the following topics:

ATTENTION
This appendix provides an example of a very basic logon script to launch the Nortel SNAS portal page. The simple script launches the end user's browser every time the user logs on, regardless of connection method. It is beyond the scope of this document to show additional examples of scripts that accommodate different modes of connecting to a Nortel SNAS port.

Configuring the logon script

To configure the logon script to automatically launch an end user's browser, perform the following steps:

Step	Action
1	Create the logon script (see "Creating a logon script" (page 502)).
2	On a Windows 2000 domain controller, save the script to the following directory: %systemroot% \ SYSVOL \ sysvol \ [Domain Name] \ Policies \ [GUID] \ User \ Scripts \ Logon

where:

- %systemroot% is an environment variable representing the operating system root folder. By default, in a Windows 2000 operating system, the root folder is called WINNT.
- [Domain Name] represents the domain on which you will use the logon script. The same script can be used in multiple domains to accomplish the same task.
- [GUID] is a globally unique indentifier for associated group policy objects.

3 Configure the default domain policy to assign the script to all users in the domain (see "Assigning the logon script" (page 503)).

--End--

Creating a logon script

To create a logon script for use on a Windows domain controller to automatically launch an end user's browser, choose one of the following:

- "Creating the script as a batch file" (page 502)
- "Creating the script as a VBScript file" (page 503)

Creating the script as a batch file

Step	Action
1	Using Windows, open a plain text editor, such as Notepad.
2	Compose the script using the following sample format: explorer.exe https://10.10.10.1 where 10.10.10.1 is the portal Virtual IP address (pVIP) of the Nortel SNAS. **ATTENTION** As an alternative to using Explorer to launch the browser, you can replace explorer.exe with the path and file name of your default browser executable, enclosed in quotes. For example: "%programfiles%\Netscape\Netscape Browser\netscape.exe"
3	Save the file as a batch file (*.bat).

--End--

Creating the script as a VBScript file

Step	Action
1	Using Windows, open a plain text editor, such as Notepad.

2	Compose the script using the following sample format:
	`Dim IE`
	`Set IE = CreateObject("InternetExplorer.Application")`
	`IE.visible = true`
	`IE.Navigate "https://10.10.10.1"`
	
	where 10.10.10.1 is the portal Virtual IP address (pVIP) of the Nortel SNAS.

3	Save the file as a VBScript file (*.vbs).

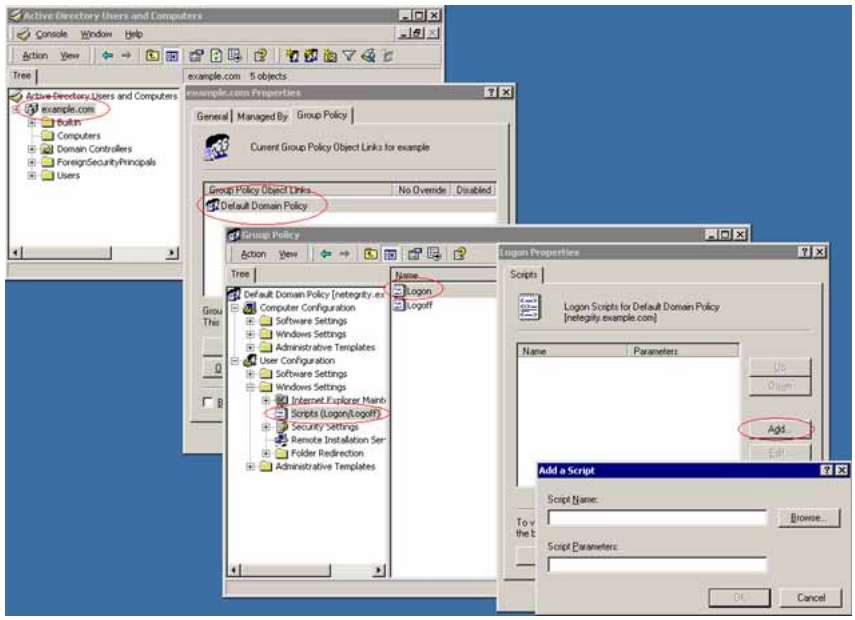
--End--

Assigning the logon script

To assign the logon script for use, perform the following steps. Figure 37 "Assigning a logon script" (page 504) illustrates the steps.

Step	Action
1	Click **Start > Administrative Tools > Active Directory Users and Computers**.
2	Right-click the domain to which you want to add the script, and select **Properties**.
3	On the Group Policy tab, click **Open**.
4	Double-click **Default Domain Policy**.
5	Right-click the Default Domain Policy and select **Edit**.
6	Expand **User Configuration > Windows Settings** and select **Scripts (Logon/Logoff)**.
7	In the right pane, double-click **Logon**.
8	Click **Add**.
9	Enter the file name of the script you want to assign, and click **OK**.
10	Click **OK**. The logon script is now assigned and will take effect the next time users log on to the domain.

Figure 37
Assigning a logon script



--End--

Appendix
Software licensing information

OpenSSL License issues

The OpenSSL toolkit stays under a dual license: both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Both licenses are actually BSD-style Open Source licenses. In case of any license issues related to OpenSSL contact openssl-core@openssl.org.

OpenSSL License Copyright © 1998-1999 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such, any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program start-up or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted, provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code), you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. That is, this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

GNU General Public License

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work that contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program," below, refers to any such program or work. A "work based on the Program" means either the Program or any derivative work under copyright law: that is, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1, above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish in whole or in part that contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it (when started running for such interactive use in the most ordinary way) to print or display an announcement, including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty), and that users may redistribute the program under these conditions, and telling the user how to view a copy

of this License. (Exception: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to the work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2, above, provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party (for a charge no more than your cost of physically performing source distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2, above, on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accordance with Subsection b, above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated

interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute, or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment, or allegation of patent infringement, or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid

or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system. It is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version," you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs in which distribution conditions are different, write to the author for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

12. IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org)". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED \Q\QAS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Bouncy Castle license

Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Index

C

D

E

F

G

H

I

O

P

Q

R

S

T

U

V

W

Y

Nortel Secure Network Access Switch

Using the Command Line Interface

Release: 2.0
Publication: NN47230-100
Document status: Standard
Document revision: 03.01
Document release date: 28 July 2008

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com
Sourced in Canada, the United States of America, and India

NORTEL